NVIDIA

Towards robust AI in healthcare without jeopardizing patient privacy

Dr. Seyed-Ahmad Ahmadi
NVIDIA Senior Solution Architect, Deep Learning in Healthcare

Workshop “Responsible ML for Healthcare”
Oct 27, 2022, Copenhagen, DK

PIONEER CENTRE FOR ARTIFICIAL INTELLIGENCE

DANMARKS FRIE FORSKNINGSFOND

DDSA

> Into whatsoever houses I enter, I will enter to help the sick, and I will abstain from all intentional wrong-doing and harm. [...]
>
> And whatsoever I shall see or hear in the course of my profession, [...] I will never divulge, **holding such things to be holy secrets**.

The Hippocratic Oath, 400 BC

Sharing is Caring:
No Learning Without Data

Federated Learning:
Learning Without Sharing Data

Data Generation:
Learning From Synthetic Data

Sharing is Caring:
No Learning Without Data

Feeding the beast: Modern ML/DL is data-hungry!

CHARITÉ UNIVERSITÄTSMEDIZIN BERLIN
MAYO CLINIC
Guy's and St Thomas' NHS Foundation Trust
Kitware
NIH NATIONAL CANCER INSTITUTE
Stanford University
UNITED IMAGING
aws
dkfz.
Google Cloud
TUM Technische Universität München
SFL SCIENTIFIC DISCOVER MORE
SNAC
Frederick National Laboratory for Cancer Research
Mass General Brigham
Children's Hospital of Philadelphia
VANDERBILT UNIVERSITY
BAYER
KING'S College LONDON
AI CENTRE for Value Based Healthcare
quantiphi
Microsoft
NVIDIA

HIPAA and GDPR

https://monai.io/

HIPAA
(Health Insurance Portability and Accountability Act)

- Since 1997: healthcare providers and insurers must ensure non-disclosure of patients' healthcare information
- Sharing EHRs requires de-identification, in two ways:
  - 1) By obtaining expert certification on de-identification,
  - 2) "Safe Harbor" approach, i.e. removal of 18 different types of patient-identifying information including names, ages, addresses, email addresses, URLs, dates of service, and lots of numbers: Social Security numbers, telephone numbers, insurance IDs, and medical records identifiers
- **Once under "Safe Harbor", data is free for sharing/buying/selling by commercial parties**

https://hai.stanford.edu/news/de-identifying-medical-patient-data-doesnt-protect-our-privacy

GDPR
(General Data Protection Regulation)

- Basic GDPR Definitions
  - Personal data: identifiable patient information
  - Pseudonymous data: data not attributable to a specific data subject, without the use of additional information
  - Anonymous data: no connection to a specific identifiable person, not even through linking to other datasets
- Both directly identifiable and pseudonymized data used by researchers should be treated as personal data
- **Processing of personal (incl pseudonymous!) data is forbidden except for patient consent (no opt-out allowed)**
- Fear of legal/social sanctions and huge penalties for violating GDPR: scientists have become reluctant to exchange data and bio-samples for secondary research
  - Hinders swift and safe data exchange in emergencies (Zika, Ebola, Covid-19)

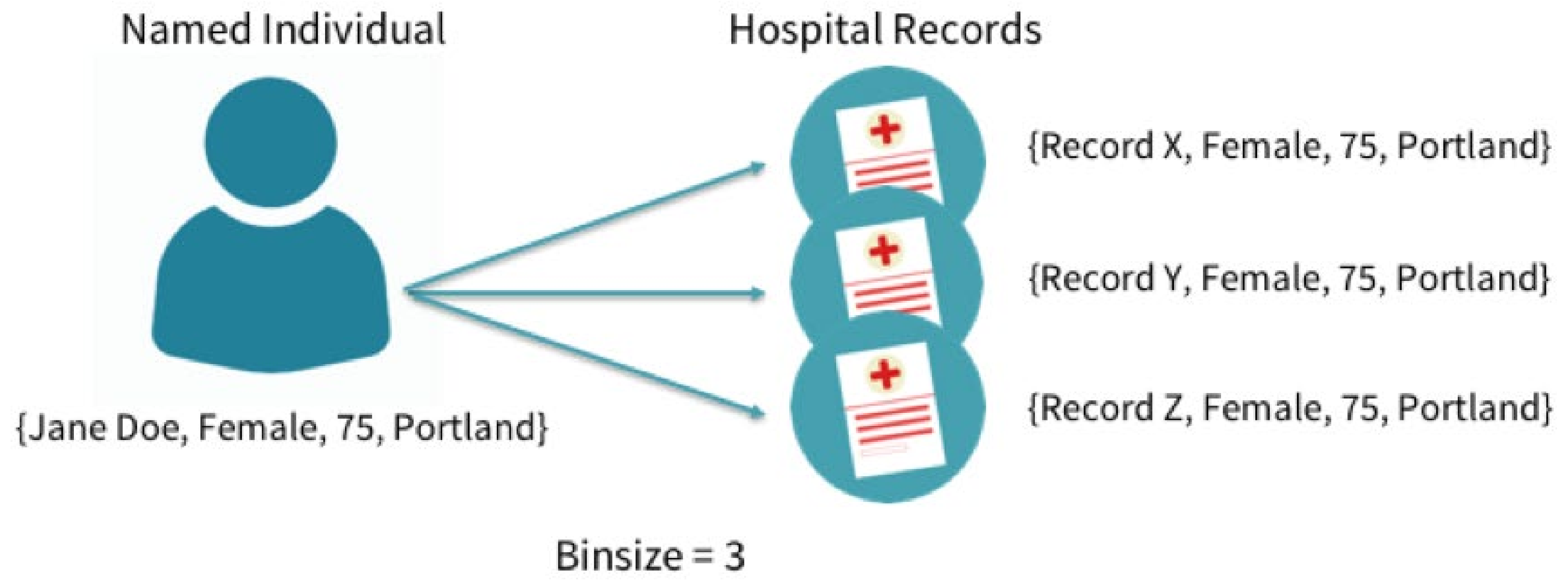
Vlahou, A., Hallinan, D., Apweiler, et al. (2021).
Data Sharing Under the General Data Protection Regulation.
In Hypertension (Vol. 77, Issue 4, pp. 1029–1035)
https://doi.org/10.1161/hypertensionaha.120.16340

Example: Patient Re-Identification from EHR Data

Cross-linking EHR data to newspaper articles

- Combining anonymized data with sparse public knowledge (e.g. public likes/tweets/shares/comments, telephone/address books)
- Very little background data is needed to de-anonymize records:
  - “We used newspaper data to match names to anonymized patient records in statewide hospital data from Maine and Vermont”
  - “When redacted to the HIPAA Safe Harbor standard, the **Maine data allowed for a 3.2 percent re-identification** rate and **Vermont data allowed for a 10.6 percent re-identification** rate.”

Maine	NewsData	HospitalData
Demographics	Name	--
	19-year-old	Age: 19
	Female	Gender: F
	Bangor, Maine	Geocode: 19020
Hospital Information	York Hospital	HP: 200020
E-code	“hit by a car while crossing highway”	E8187 Other noncollision motor vehicle traffic accident injuring pedestrian
Diagnoses	“two broken bones in right leg, bruises to arms, legs, suffered head injuries”	87344 Open wound of jaw, without mention of complication
		82380 Closed fracture of unspecified part of tibia alone
		8249 Unspecified fracture of ankle, open
		88101 Open wound of elbow, without mention of complication
Sensitive information unrelated to hospitalization included in HospitalData		311 Depressive disorder
		30981 Posttraumatic stress disorder
		30000 Anxiety state



- Eman & Arbuckly propose a max. re-identification risk of of < 0.5 or 0.3
- i.e. each record should be matched with at least two or three others.

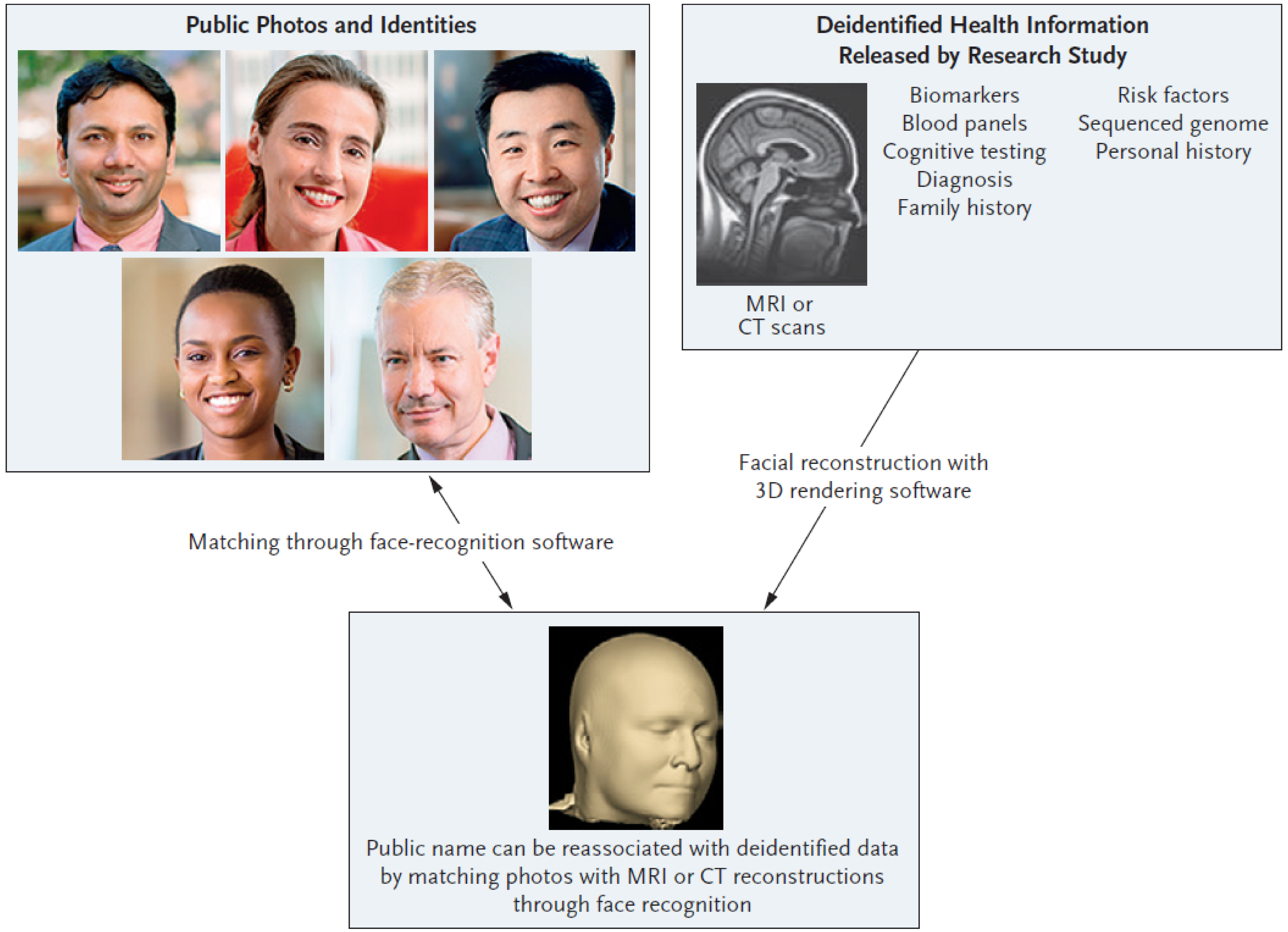
Khaled El Emam and Luk Arbuckle. 2013. Anonymizing Health Data: Case Studies and Methods to Get You Started (1st. ed.). O'Reilly Media, Inc.

Yoo J, Thaler A, Sweeney L, Zang J. Risks to Patient Privacy: A Re-identification of Patients in Maine and Vermont Statewide Hospital Data. Technology Science. 2018100901. Oct 08, 2018. https://techscience.org/a/2018100901/

Example: Patient Re-Identification from Medical Images

Facial Recognition by combining MRIs and Public Databases

A



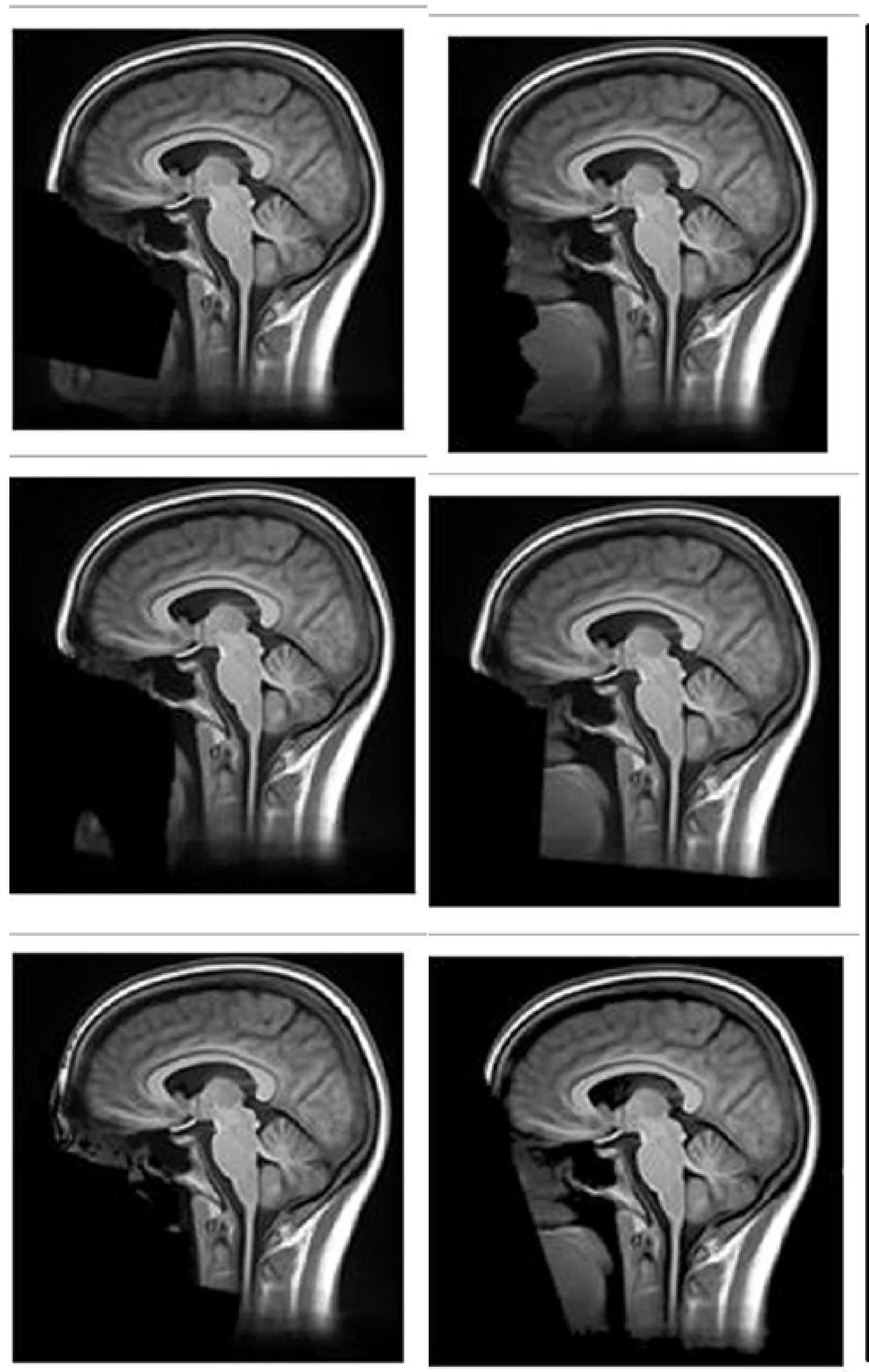
B

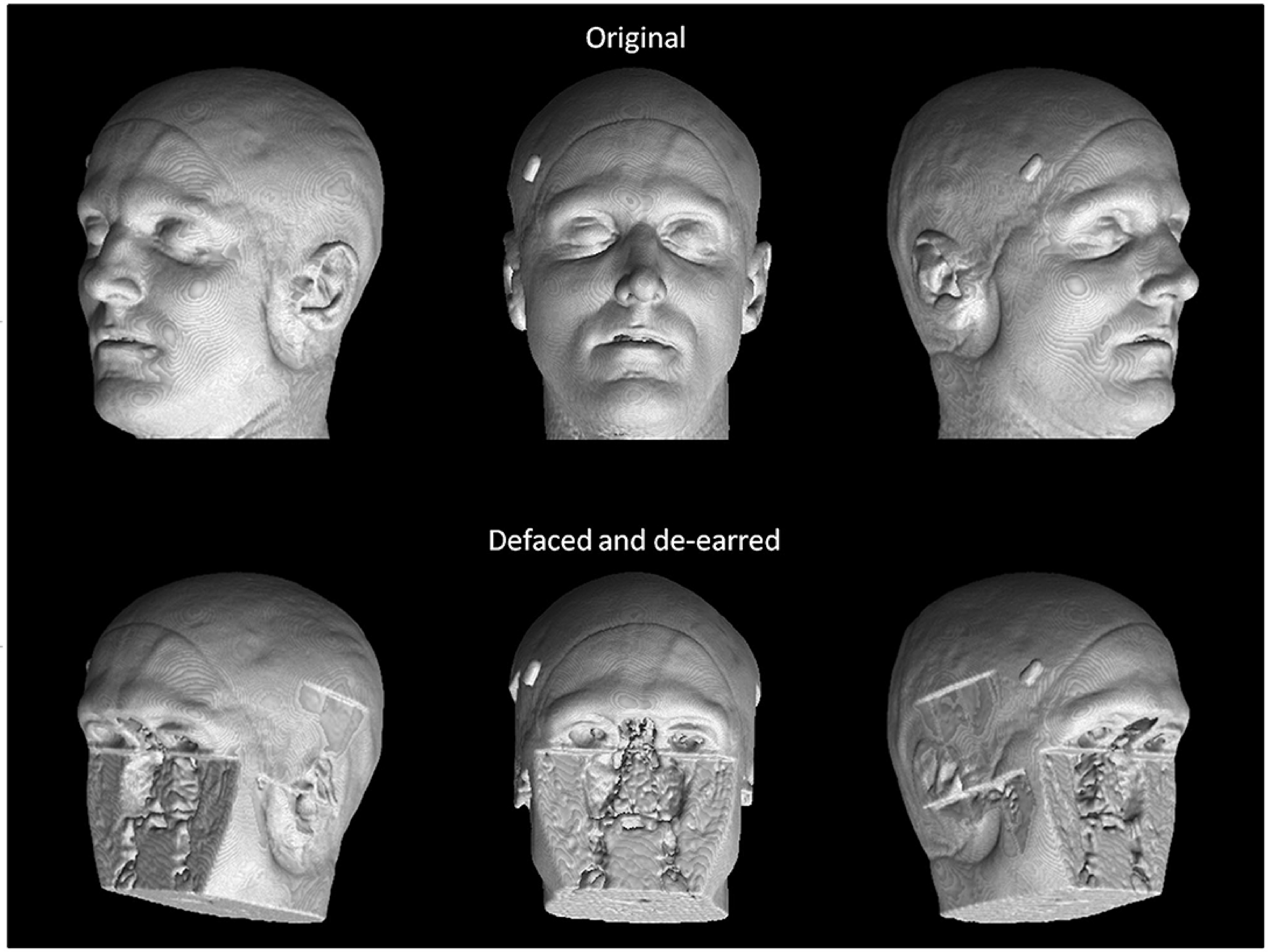
Schwarz, C. G., Kremers, W. K., Therneau, T. M., Sharp, R. R., Gunter, J. L., Vemuri, P., Arani, A., Spychalla, A. J., Kantarci, K., Knopman, D. S., Petersen, R. C., & Jack, C. R., Jr. (2019). Identification of Anonymous MRI Research Participants with Face-Recognition Software. In New England Journal of Medicine (Vol. 381, Issue 17, pp. 1684–1686). Massachusetts Medical Society. https://doi.org/10.1056/nejmc1908881

Example: Advanced De- and Re-Identification

Facial Recognition: Is De-Facing enough?

Various de-facing methods…





…vs Brainprint

"BrainPrint captures unique information about the subject's anatomy and permits to correctly classify a scan with an accuracy of over 99.8%"

Theyers et al., Multisite Comparison of MRI Defacing Software Across Multiple Cohorts, Front. Psychiatry, 24 February 2021, https://doi.org/10.3389/fpsyt.2021.617997

Wachinger, C., Golland, P., & Reuter, M., BrainPrint : Identifying Subjects by Their Brain. In MICCAI 2014 (pp. 41–48), Springer, https://doi.org/10.1007/978-3-319-10443-0_6

Federated Learning (FL): Fundamentals & NVIDIA FLARE

“

FL enables gaining insights collaboratively, e.g., in the form of a consensus model, without moving patient data beyond the firewalls of the institutions in which they reside.

Rieke et al., Nature Dig. Med., 2020
https://doi.org/10.1038/s41746-020-00323-1

”

Building ai for real-world clinical performance

Taking Algorithms Beyond Proof-of-Concept

REAL-WORLD AI DESIGN

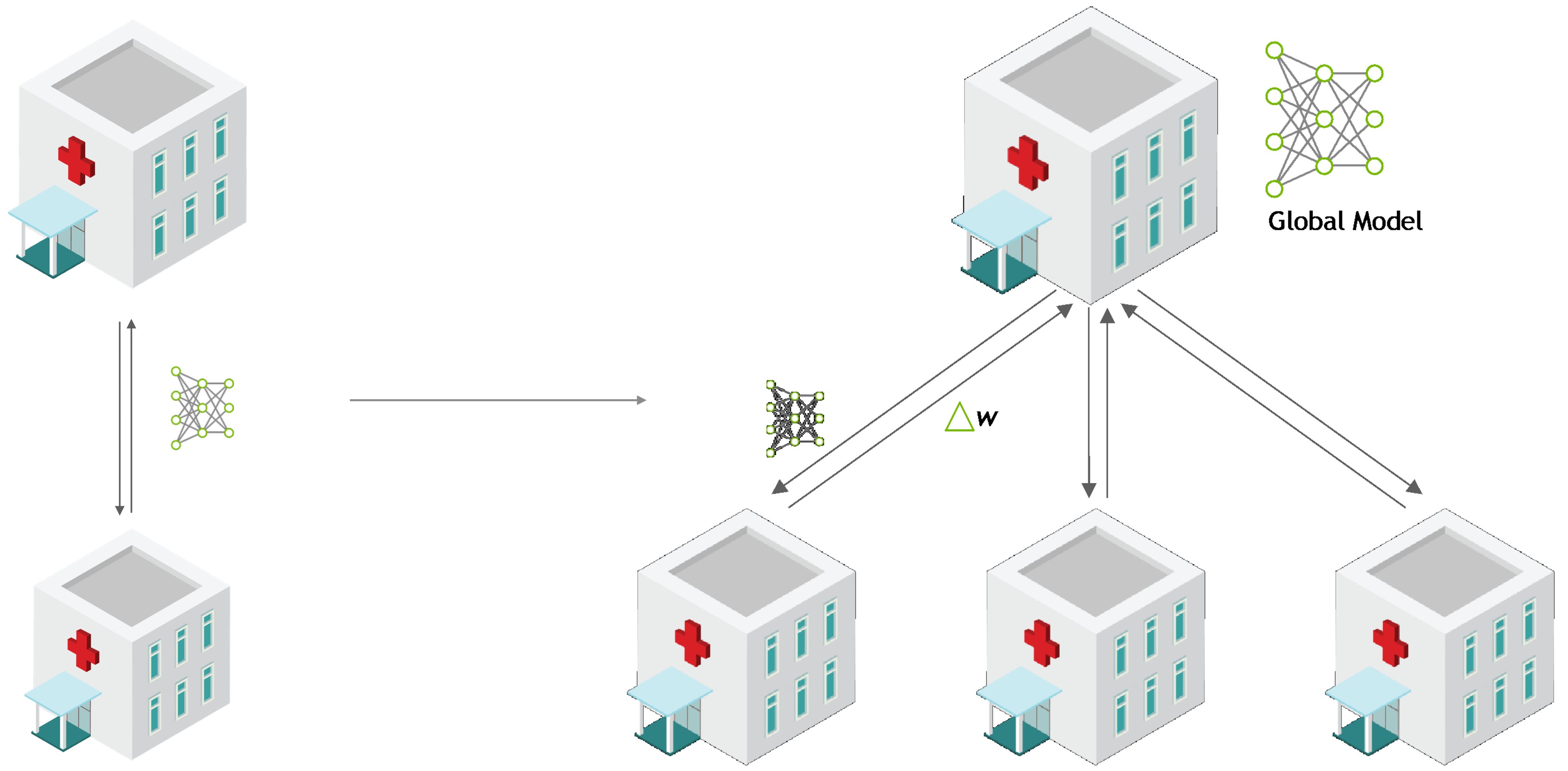
External Validation, Multiple Institutions, Prospective Data

Design Characteristic	All Articles (n = 516)	Articles Published in Medical Journals (n = 437)
External validation		
Used	31 (6.0)	27 (6.2)
Not used	485 (94.0)	410 (93.8)
In studies that used external validation		
Diagnostic cohort design	5 (1.0)	5 (1.1)
Data from multiple institutions	15 (2.9)	12 (2.7)
Prospective data collection	4 (0.8)	4 (0.9)
Fulfillment of all of above three criteria	0 (0)	0 (0)
Fulfillment of at least two criteria	3 (0.6)	3 (0.7)
Fulfillment of at least one criterion	21 (4.1)	18 (4.1)

Only 6% of published AI studies have external validation
Few included multiple institutions

FEDERATED LEARNING PARADIGM

Model to Data | Generalize Model



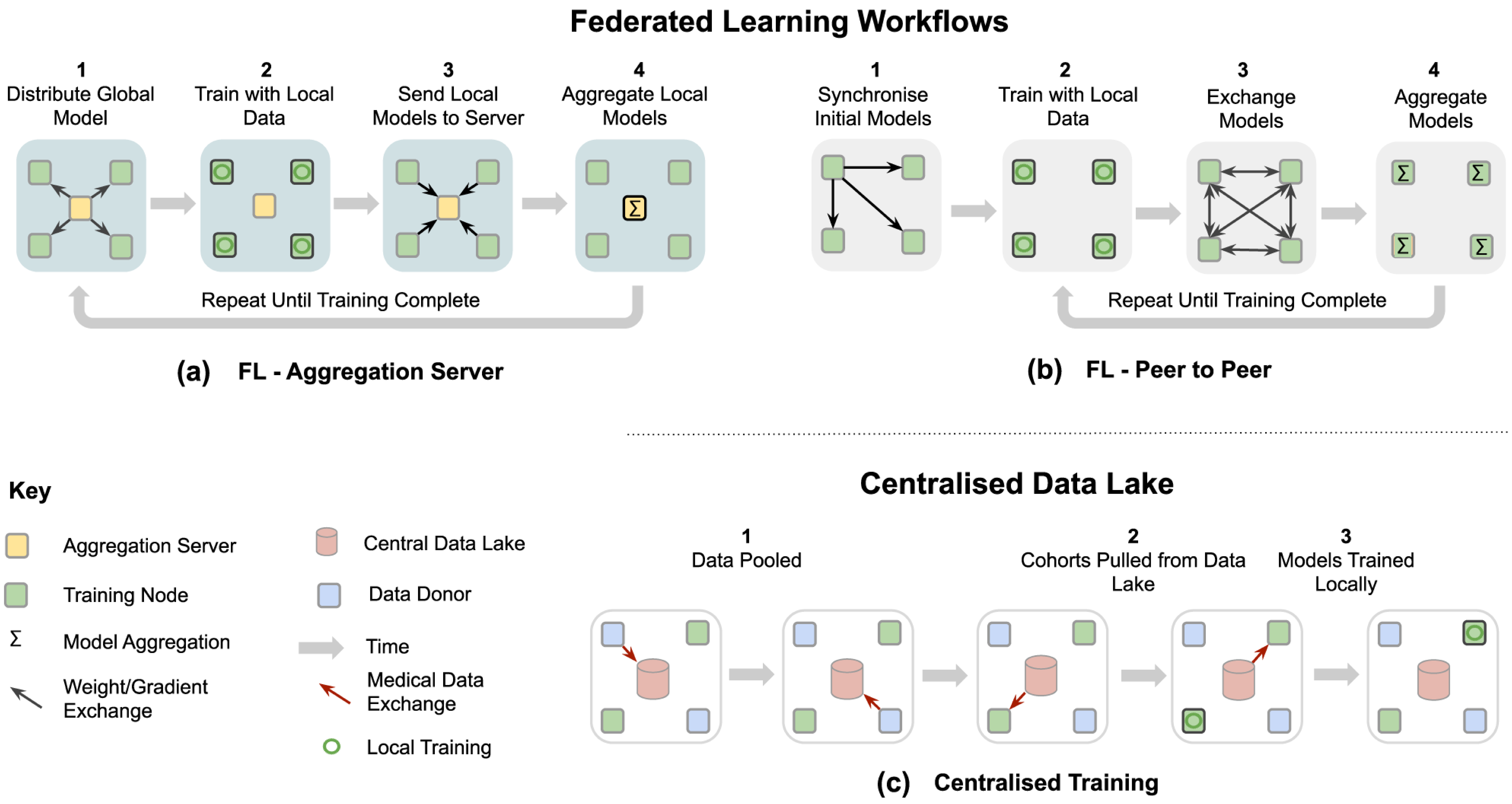
Transfer Learning
"Adapt"

Federated Learning
"Generalize"

Kim DW, Jang HY, Kim KW, Shin Y, Park SH. Design Characteristics of Studies Reporting the Performance of Artificial Intelligence Algorithms for Diagnostic Analysis of Medical Images: Results from Recently Published Papers. Korean J Radiol. 2019 Mar;20(3):405-410. doi: 10.3348/kjr.2019.0025. PMID: 30799571; PMCID: PMC6389801.

Federated Learning Workflows

Difference to Learning on a Centralised Data Lake

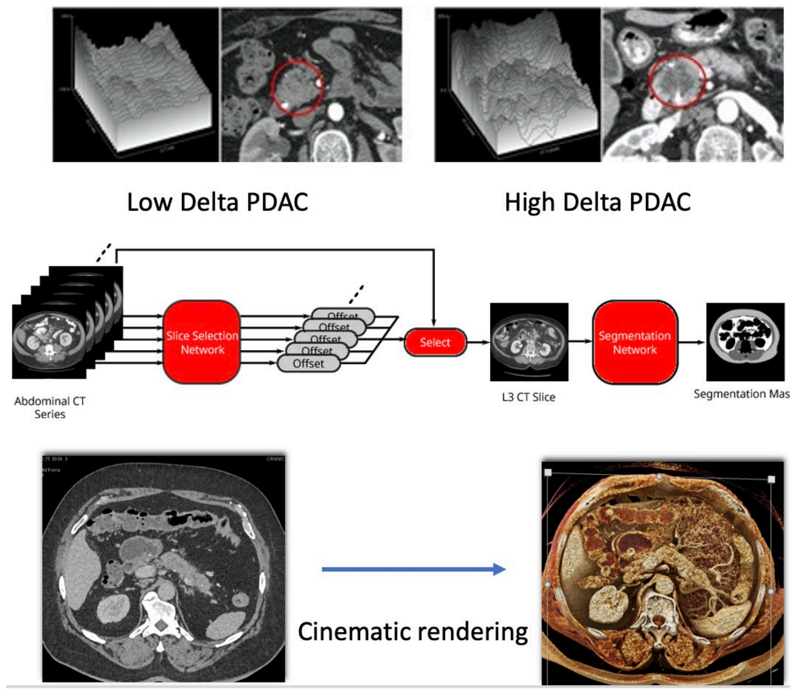


Rieke, N., Hancox, J., Li, W. *et al.* The future of digital health with federated learning. *npj Digit. Med.* **3**, 119 (2020). https://doi.org/10.1038/s41746-020-00323-1

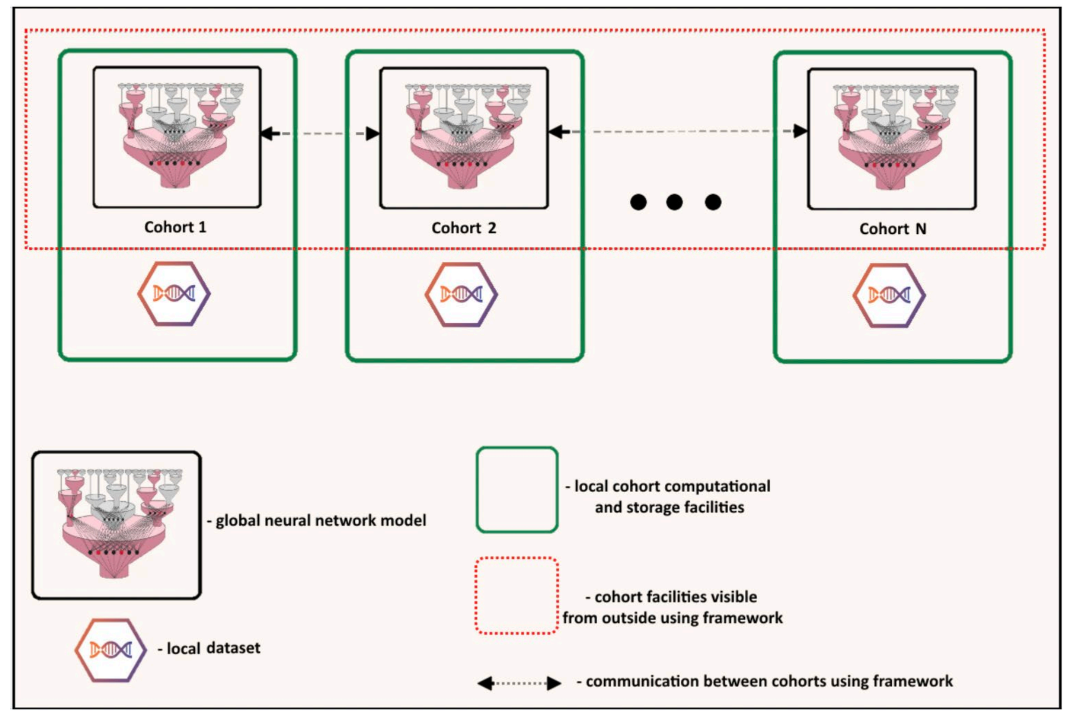
Federated learning MOMENTUM

Breaking Healthcare Data Siloes

EDRN
Early Detection of Pancreatic Cancer



ERASMUS GENNET
Genome Wide Association Study



EXAM
COVID-19 Oxygen Requirement Prediction

nature medicine

ARTICLES

https://doi.org/10.1038/s41591-021-01506-3

Check for updates

Federated learning for predicting clinical outcomes in patients with COVID-19

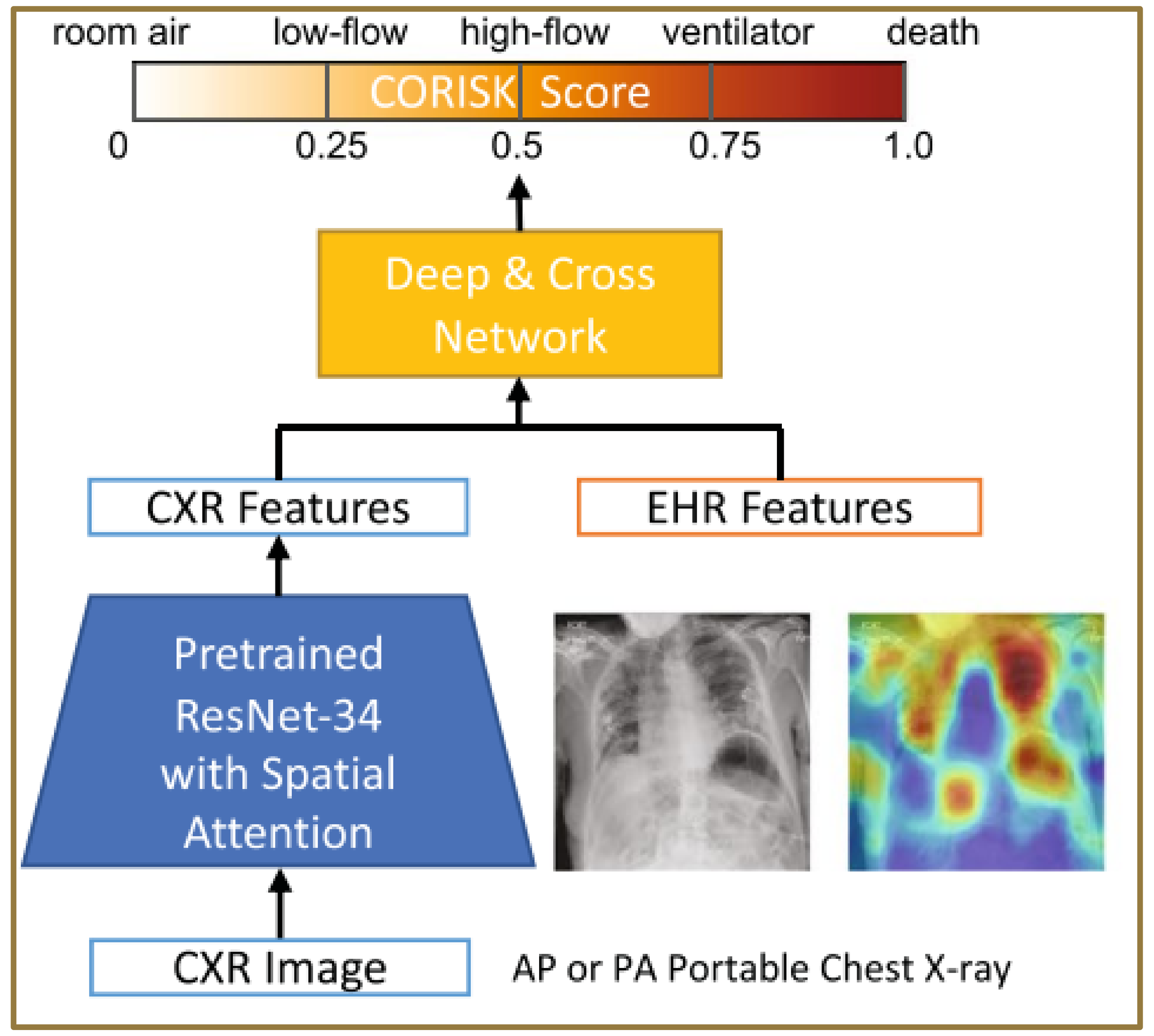
Ittai Dayan[1,56], Holger R. Roth[2,56], Aoxiao Zhong[3,4,56], Ahmed Harouni[2], Amilcare Gentili[5], Anas Z. Abidin[2], Andrew Liu[2], Anthony Beardsworth Costa[6], Bradford J. Wood[7,8], Chien-Sung Tsai[9], Chih-Hung Wang[10,11], Chun-Nan Hsu[12], C. K. Lee[2], Peiying Ruan[2], Daguang Xu[2], Dufan Wu[3], Eddie Huang[2], Felipe Campos Kitamura[13], Griffin Lacey[2], Gustavo César de Antônio Corradi[13], Gustavo Nino[14], Hao-Hsin Shin[15], Hirofumi Obinata[16], Hui Ren[3], Jason C. Crane[17], Jesse Tetreault[2], Jiahui Guan[2], John W. Garrett[18], Joshua D. Kaggie[19], Jung Gil Park[20], Keith Dreyer[1,21], Krishna Juluru[15], Kristopher Kersten[2], Marcio Aloisio Bezerra Cavalcanti Rockenbach[21], Marius George Linguraru[22,23], Masoom A. Haider[24,25], Meena AbdelMaseeh[25], Nicola Rieke[2], Pablo F. Damasceno[17], Pedro Mario Cruz e Silva[2], Pochuan Wang[26,27], Sheng Xu[7,8], Shuichi Kawano[16], Sira Sriswasdi[28,29], Soo Young Park[30], Thomas M. Grist[31], Varun Buch[21], Watsamon Jantarabenjakul[32,33], Weichung Wang[26,27], Won Young Tak[30], Xiang Li[3], Xihong Lin[34], Young Joon Kwon[6], Abood Quraini[2], Andrew Feng[2], Andrew N. Priest[35], Baris Turkbey[8,36], Benjamin Glicksberg[37], Bernardo Bizzo[21], Byung Seok Kim[38], Carlos Tor-Díez[22], Chia-Cheng Lee[39], Chia-Jung Hsu[39], Chin Lin[40,41,42], Chiu-Ling Lai[43], Christopher P. Hess[17], Colin Compas[2], Deepeksha Bhatia[2], Eric K. Oermann[44], Evan Leibovitz[21], Hisashi Sasaki[16], Hitoshi Mori[16], Isaac Yang[2], Jae Ho Sohn[17], Krishna Nand Keshava Murthy[15], Li-Chen Fu[45], Matheus Ribeiro Furtado de Mendonça[13], Mike Fralick[46], Min Kyu Kang[20], Mohammad Adil[2], Natalie Gangai[15], Peerapon Vateekul[47], Pierre Elnajjar[15], Sarah Hickman[19], Sharmila Majumdar[17], Shelley L. McLeod[48,49], Sheridan Reed[7,8], Stefan Gräf[50], Stephanie Harmon[8,51], Tatsuya Kodama[16], Thanyawee Puthanakit[32,33], Tony Mazzulli[52,53,54], Vitor Lima de Lavor[13], Yothin Rakvongthai[55], Yu Rim Lee[30], Yuhong Wen[2], Fiona J. Gilbert[19,56], Mona G. Flores[2,56] ✉ and Quanzheng Li[3,56]

Federated learning (FL) is a method used for training artificial intelligence models with data from multiple sources while maintaining data anonymity, thus removing many barriers to data sharing. Here we used data from 20 institutes across the globe to train a FL model, called EXAM (electronic medical record (EMR) chest X-ray AI model), that predicts the future oxygen requirements of symptomatic patients with COVID-19 using inputs of vital signs, laboratory data and chest X-rays. EXAM achieved an average area under the curve (AUC) >0.92 for predicting outcomes at 24 and 72 h from the time of initial presentation to the emergency room, and it provided 16% improvement in average AUC measured across all participating sites and an average increase in generalizability of 38% when compared with models trained at a single site using that site's data. For prediction of mechanical ventilation treatment or death at 24 h at the largest independent test site, EXAM achieved a sensitivity of 0.950 and specificity of 0.882. In this study, FL facilitated rapid data science collaboration without data exchange and generated a model that generalized across heterogeneous, unharmonized datasets for prediction of clinical outcomes in patients with COVID-19, setting the stage for the broader use of FL in healthcare.

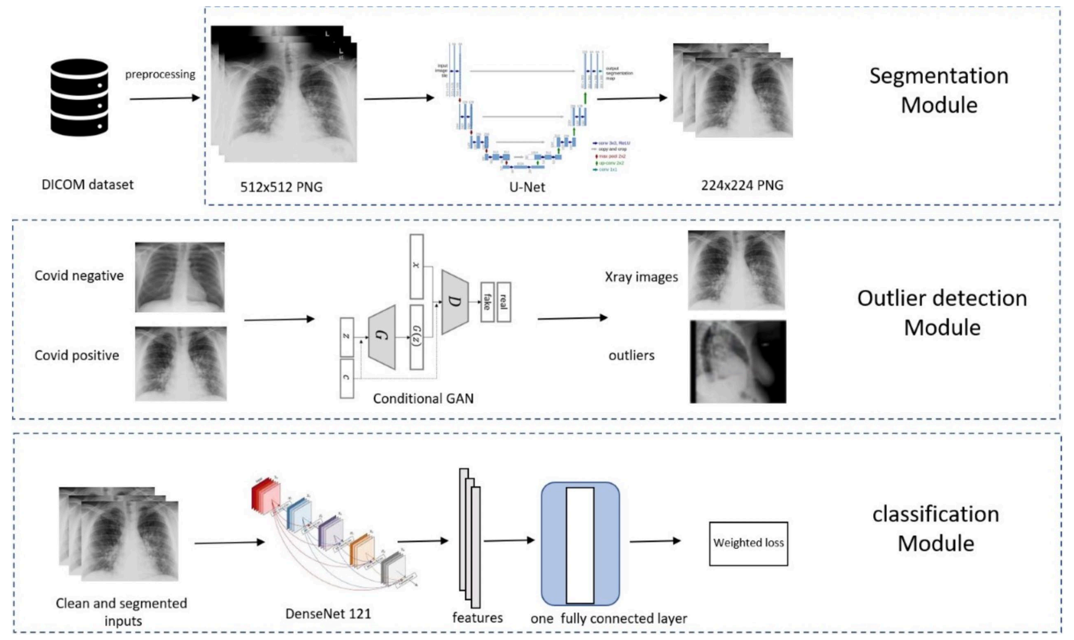
The scientific, academic, medical and data science communities have come together in the face of the COVID-19 pandemic crisis to rapidly assess novel paradigms in artificial intelligence (AI) that are rapid and secure, and potentially incentivize data sharing and model training and testing without the usual privacy and data ownership hurdles of conventional collaborations[1,2]. Healthcare providers, researchers and industry have pivoted their focus to address unmet and critical clinical needs created by the crisis, with remarkable results[3–9]. Clinical trial recruitment has been expedited and facilitated by national regulatory bodies and an international cooperative spirit[10–12]. The data analytics and AI disciplines have always fostered open

A full list of affiliations appears at the end of the paper.

NATURE MEDICINE | VOL 27 | OCTOBER 2021 | 1735–1743 | www.nature.com/naturemedicine 1735



U MINNESOTA, FAIRVIEW
X-RAY Covid-19 Classification



MELLODDY
Multi-task Learning Chemical Assays

PHARMA PARTNERS

AMGEN, astellas, AstraZeneca, Bayer, Boehringer Ingelheim, gsk, janssen, Merck, NOVARTIS, SERVIER

PUBLIC PARTNERS

KU LEUVEN, IKTOS, loodse, NVIDIA, OWKIN, SUBSTRA

NVIDIA Federated Learning

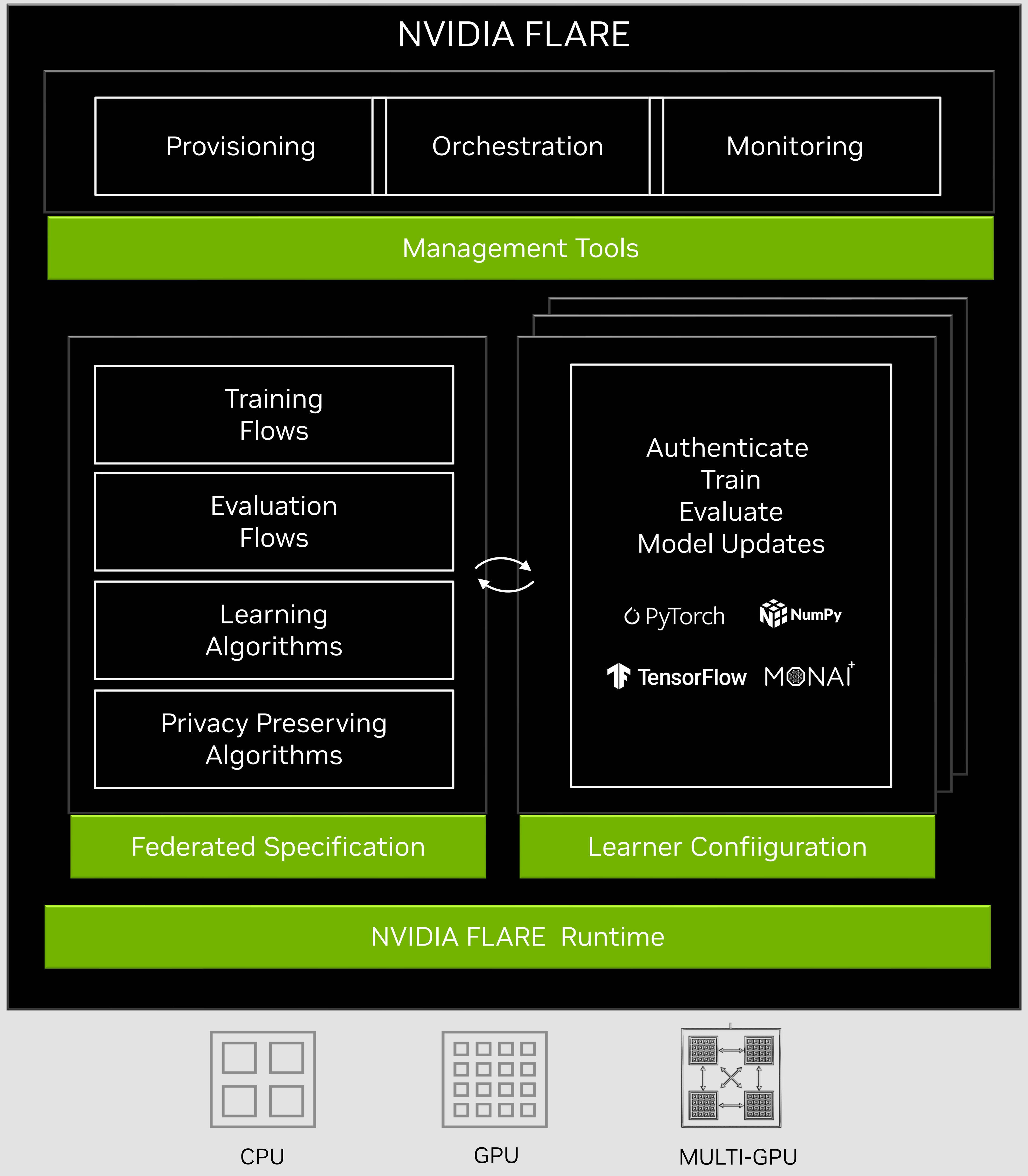
Applications across industries

Nvidia FLARE

Open-Source SDK for Federated Learning

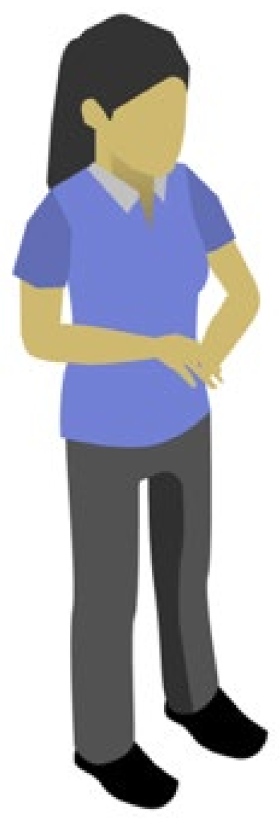
- Apache License 2.0 to catalyze FL research & development
- Enables Distributed, Multi-Party Collaborative Learning
- Adapt existing ML/DL workflows to a Federated paradigm
- Privacy Preserving Algorithms
  - Homomorphic Encryption & Differential Privacy
- Secure Provisioning, Orchestration & Monitoring
- Programmable APIs for Extensibility

Available on Github: https://github.com/nvidia/nvFlare



PERSONAS (WHO & VALUE PROP FOR EACH)

FL RESEARCHERS



Enables ease of getting started with FL experiments execution & evaluation in real world.

Extensible APIs for ease of creating custom implementations for new federated workflows, learning & privacy preserving algorithms.

DATA SCIENTISTS

Extend existing DL/ML workflows with a Federated paradigm and explore potential of Federated learning.

Ready to use FL specification and management tools enabling seamless execution.

PLATFORM DEVELOPERS

A robust, extensible foundation to customize a platform offering for end users.

Built-in implementations of Federated learning spec & Aux APIs to build custom offerings.

NVIDIA FLARE KEY CAPABILITIES

Runtime-ready and extensible suite of features

Privacy-Preserving Algorithms

NVIDIA FLARE provides privacy-preserving algorithms that ensure each change to the global model stays hidden and prevent the server from reverse-engineering the submitted weights and discovering any training data.

Training and Evaluation Workflows

Built-in workflow paradigms use local and decentralized data to keep models relevant at the edge, including learning algorithms for FedAvg, FedOpt, and FedProx.

Extensible Management Tools

Management tools help secure provisioning using SSL certifications, orchestration through an admin console, and monitoring of federated learning experiments using TensorBoard for visualization.

Supports Popular ML/DL Frameworks

Flexible in design, the SDK can be used with PyTorch, Tensorflow, and even Numpy, which allows for integrating federated learning into your current workflow.

Extensive API

Its extensive and open-source API enables researchers to develop new federated workflow strategies, innovative learning, and privacy-preserving algorithms.

Reusable Building Blocks

NVIDIA FLARE provides an easy way to perform federated learning experiments by utilizing the reusable building blocks and example walkthroughs.

https://developer.nvidia.com/flare

FLARE 2.1: Built for Scalability

High-Availability & Multi-Task Execution

- High availability (HA) supports multiple FL servers and automatically activates a backup server when the currently active server becomes unavailable.
- This is managed by a new entity in the federation, the overseer, that's responsible for monitoring the state of all participants and orchestrating the cutover to a backup server when needed.
- Multi-job execution supports resource-based multi-job execution by allowing for concurrent runs, provided that the resources required by the jobs are satisfied

https://developer.nvidia.com/blog/experimenting-with-novel-distributed-applications-using-nvidia-flare-2-1/

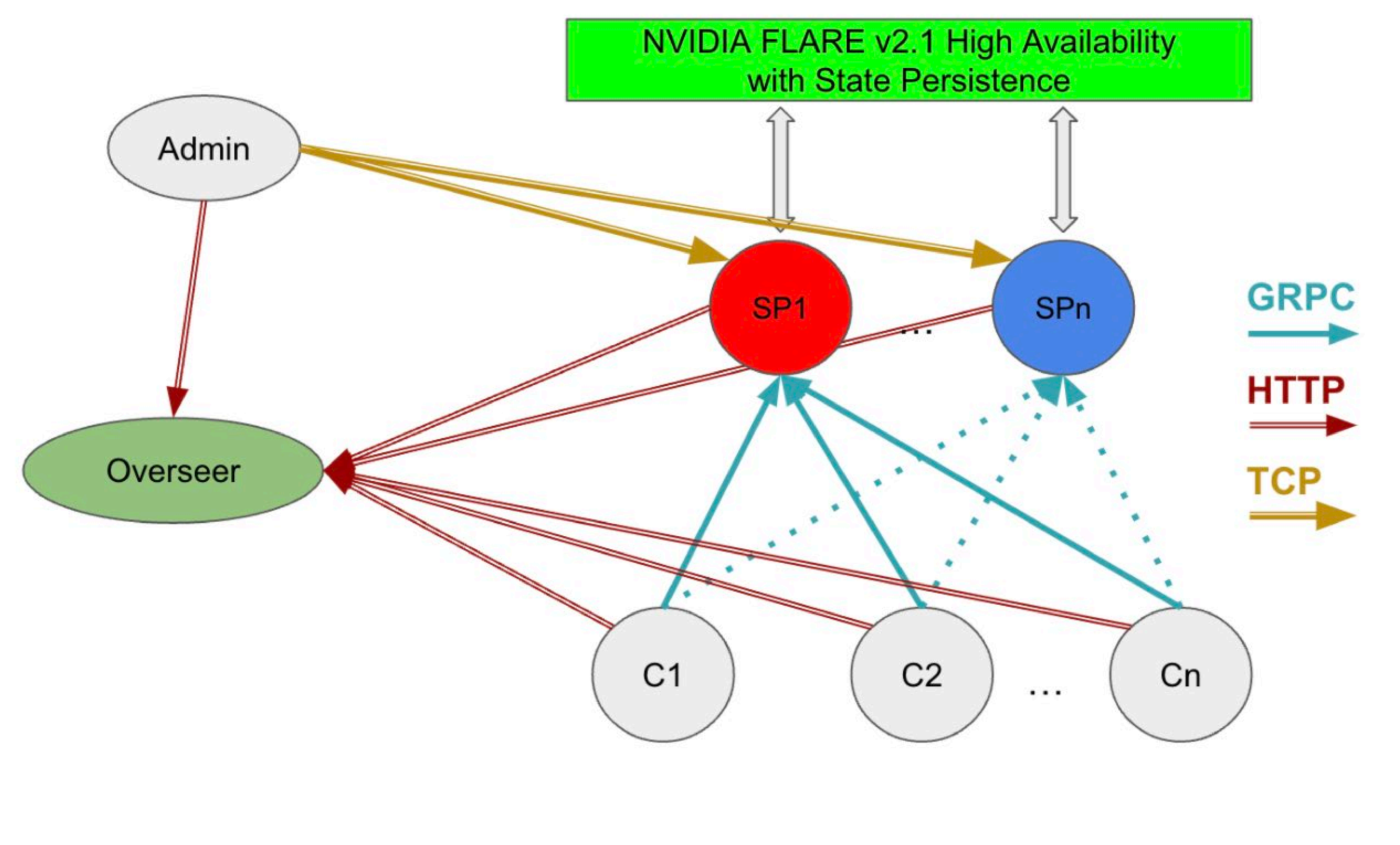


Figure 3. The NVIDIA FLARE deployment for high availability (HA)

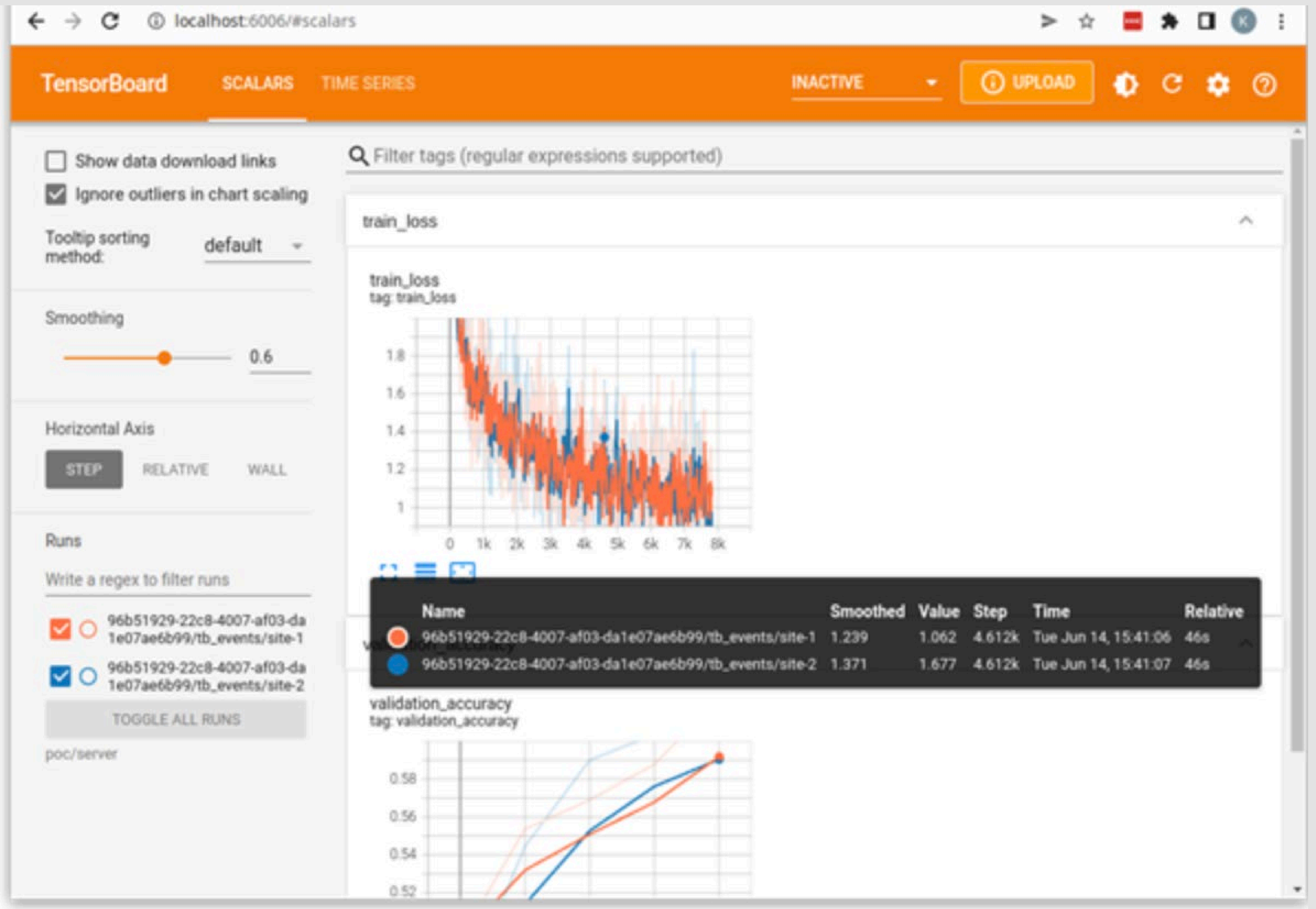


Figure 2. Example TensorBoard output from the hello-pt-tb *application*

Security & Privacy

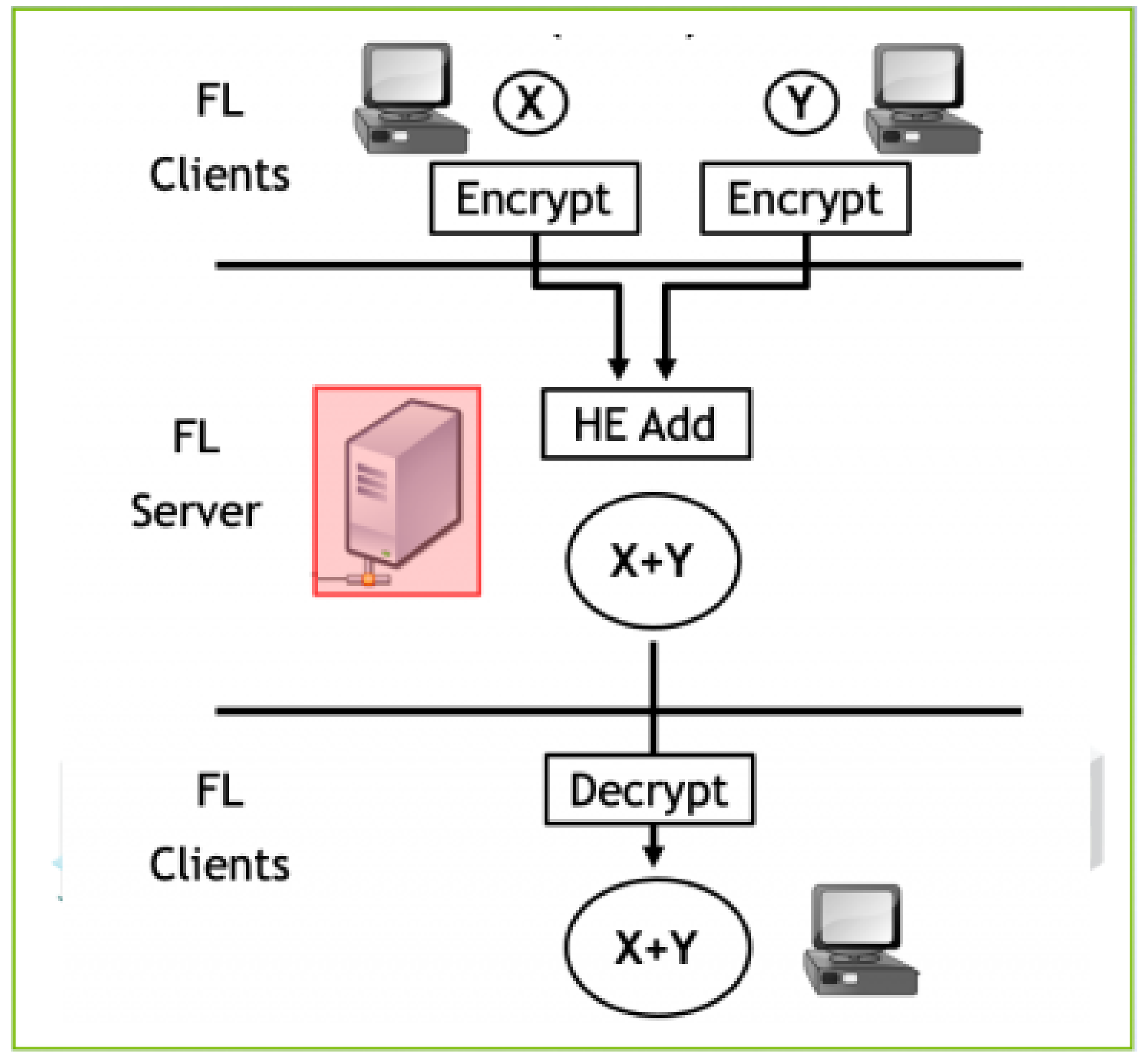
Homomorphic Encryption & Differential Privacy

Federated Learning with Homomorphic Encryption

What if I don't trust the server?

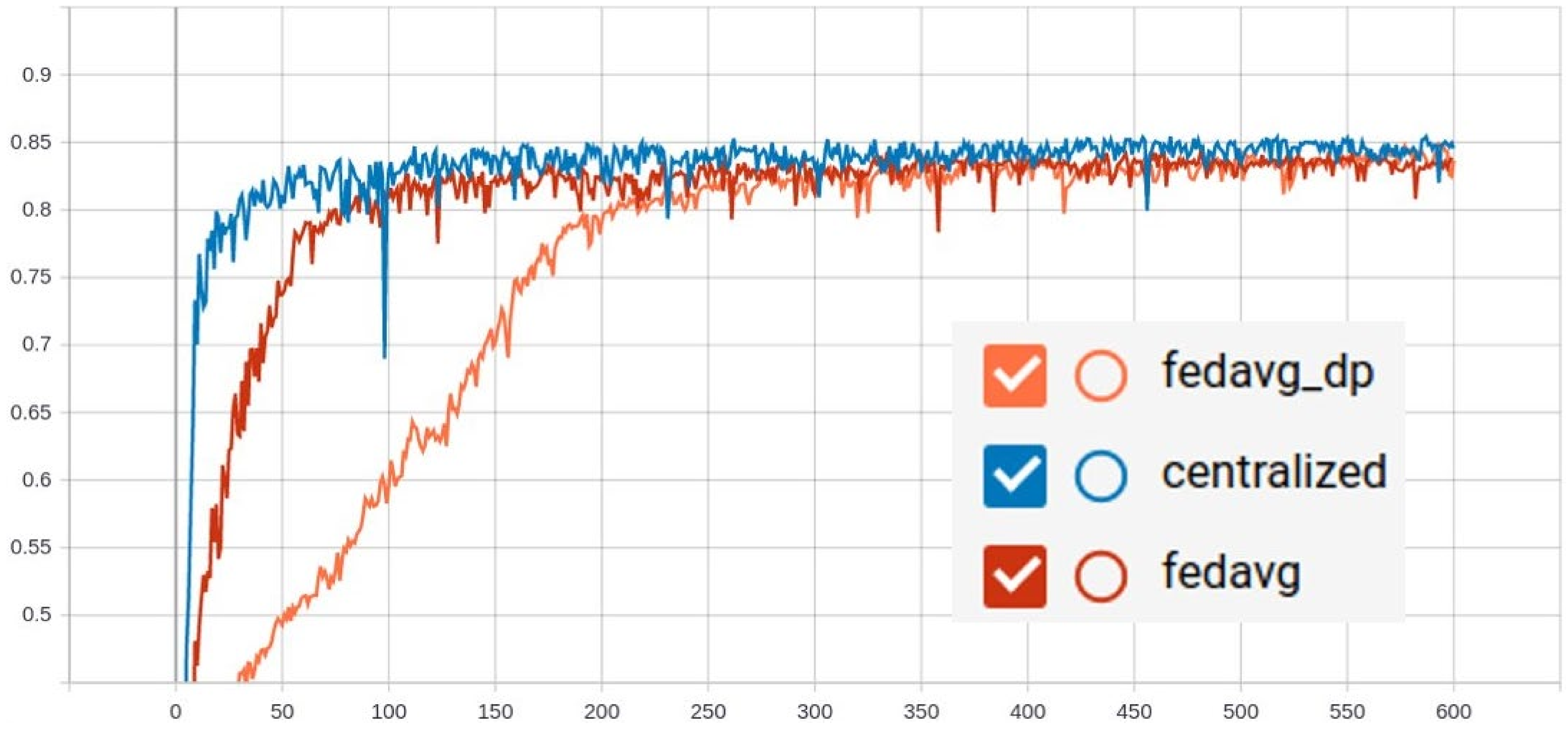
Homomorphic encryption (HE)

A form of encryption that permits users to perform computations on encrypted data



Differential Privacy for BraTS18 Segmentation

validation Dice scores of the global model for 600 training epochs:



Blog: https://developer.nvidia.com/blog/federated-learning-with-homomorphic-encryption/
Example: https://github.com/NVIDIA/NVFlare/tree/main/examples/cifar10

Example: https://github.com/NVIDIA/NVFlare/tree/main/examples/brats18

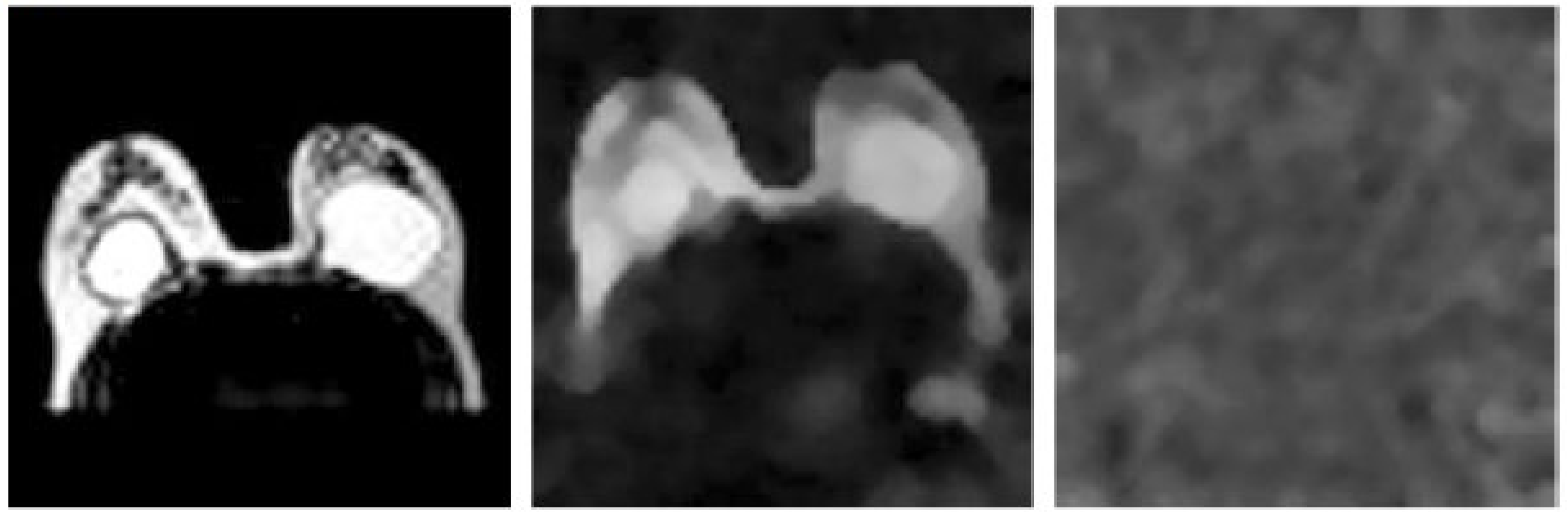
Why differential privacy?

Counter-acting gradient-based privacy attacks

a Original Without DP With DP

"Breast MRI revealing absence of the right breast, likely due to operative removal due to breast cancer"

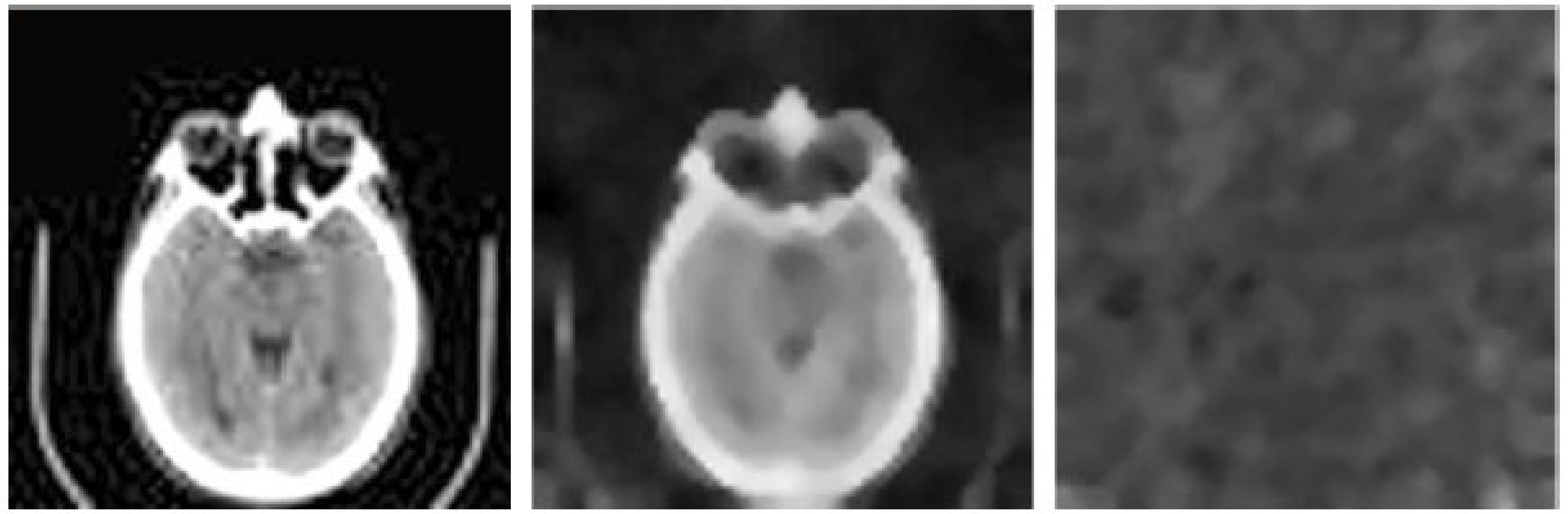
b Original Without DP With DP



"Breast MRI revealing breast implants."

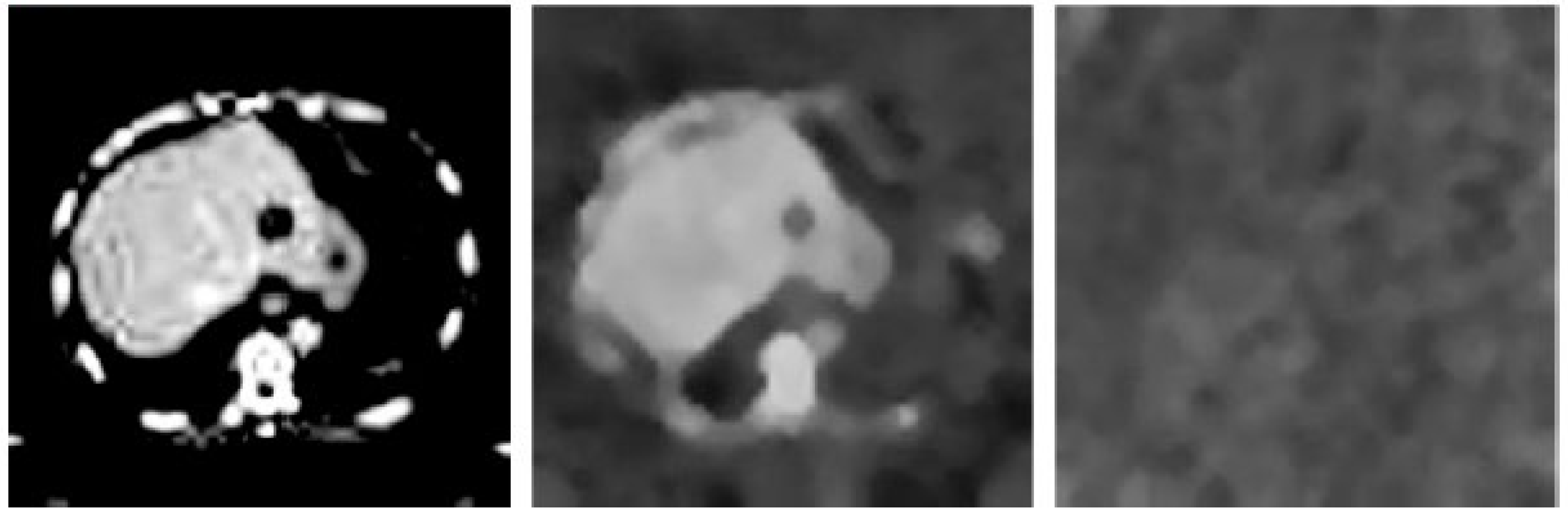
"Both a and b also allow assumptions about the patient's sex!"

c Original Without DP With DP



"Cranial computed tomography image at the level of the nose: potential for facial detection."

d Original Without DP With DP

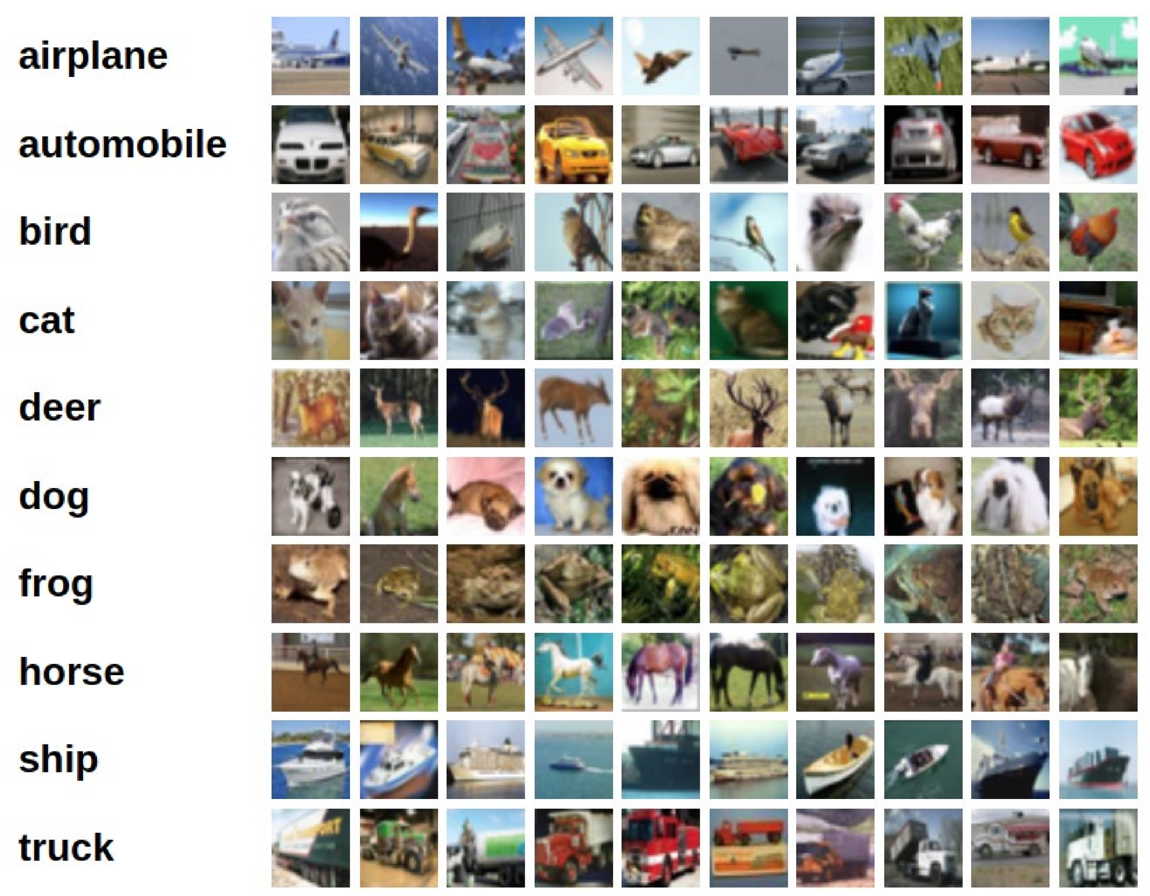


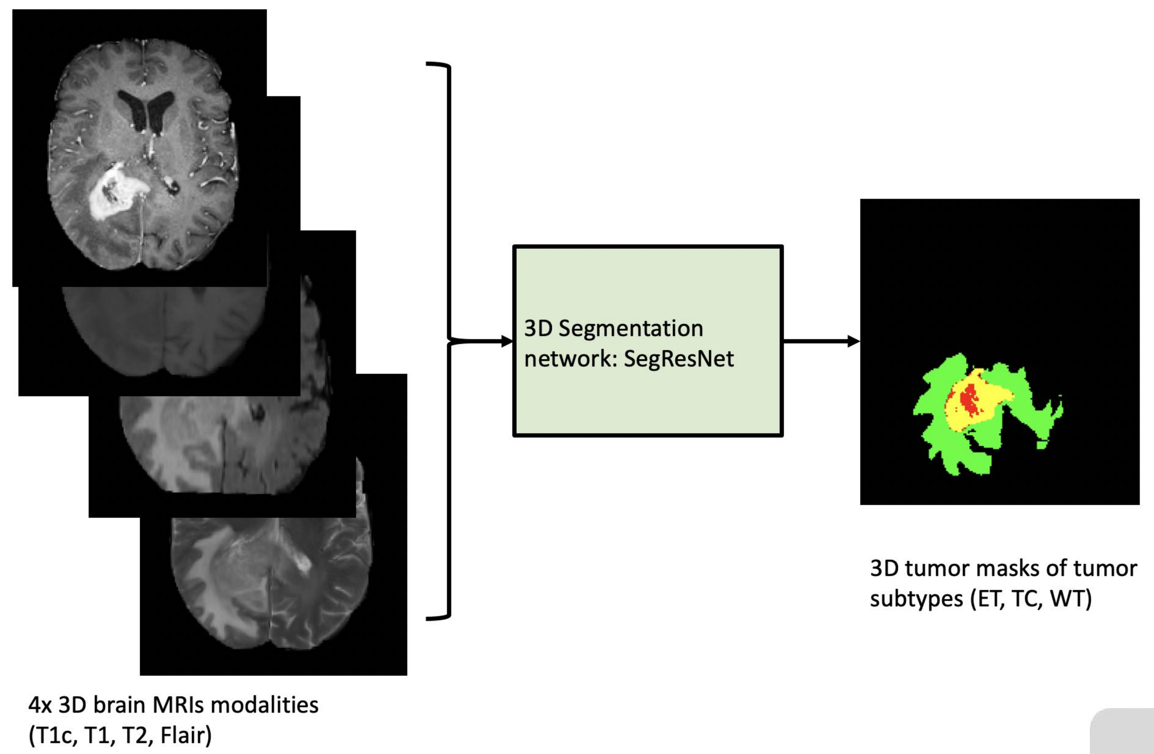
"Abdominal CT at the level of the liver, allowing visualization of a hypodense lesion in the left liver lobe in the reconstructed Image."

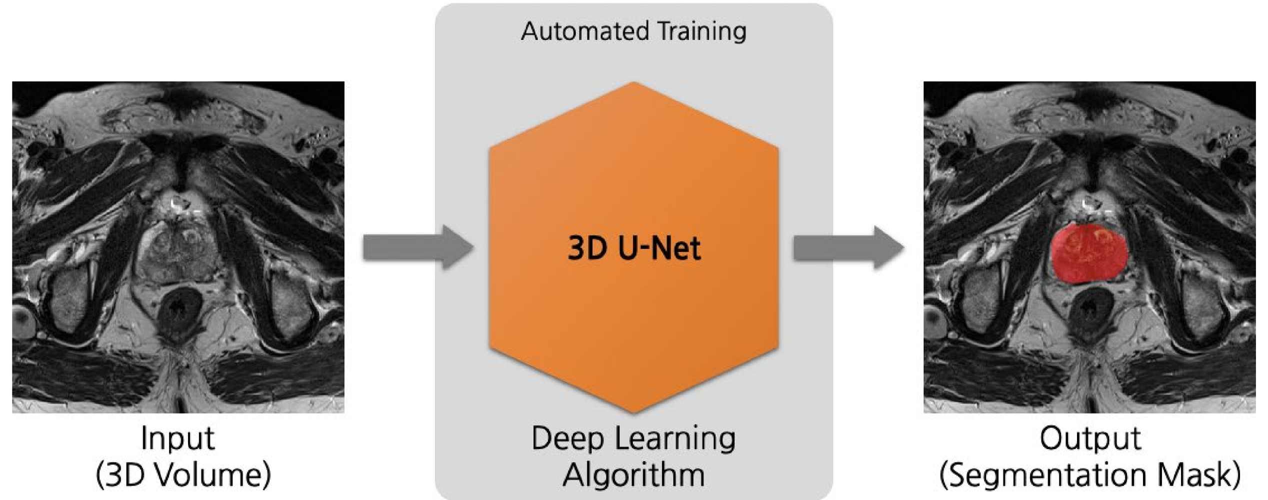
Kaissis, G., Ziller, A., Passerat-Palmbach, J. et al. End-to-end privacy preserving deep learning on multi-institutional medical imaging. Nat Mach Intell 3, 473–484 (2021). https://doi.org/10.1038/s42256-021-00337-8

End-to-end examples (CIFAR10, BRATS18, PROSTATE)

- Comprehensive example for researchers to compare algorithms
    1. Set up a virtual environment
    2. Create your FL workspace
    3. Run automated experiments
        1. Varying data heterogeneity of data splits
        2. Centralized training
        3. FedAvg on different data splits
        4. Advanced FL algorithms (FedProx and FedOpt)
        5. Secure aggregation using homomorphic encryption
        6. Differential privacy
    4. Results



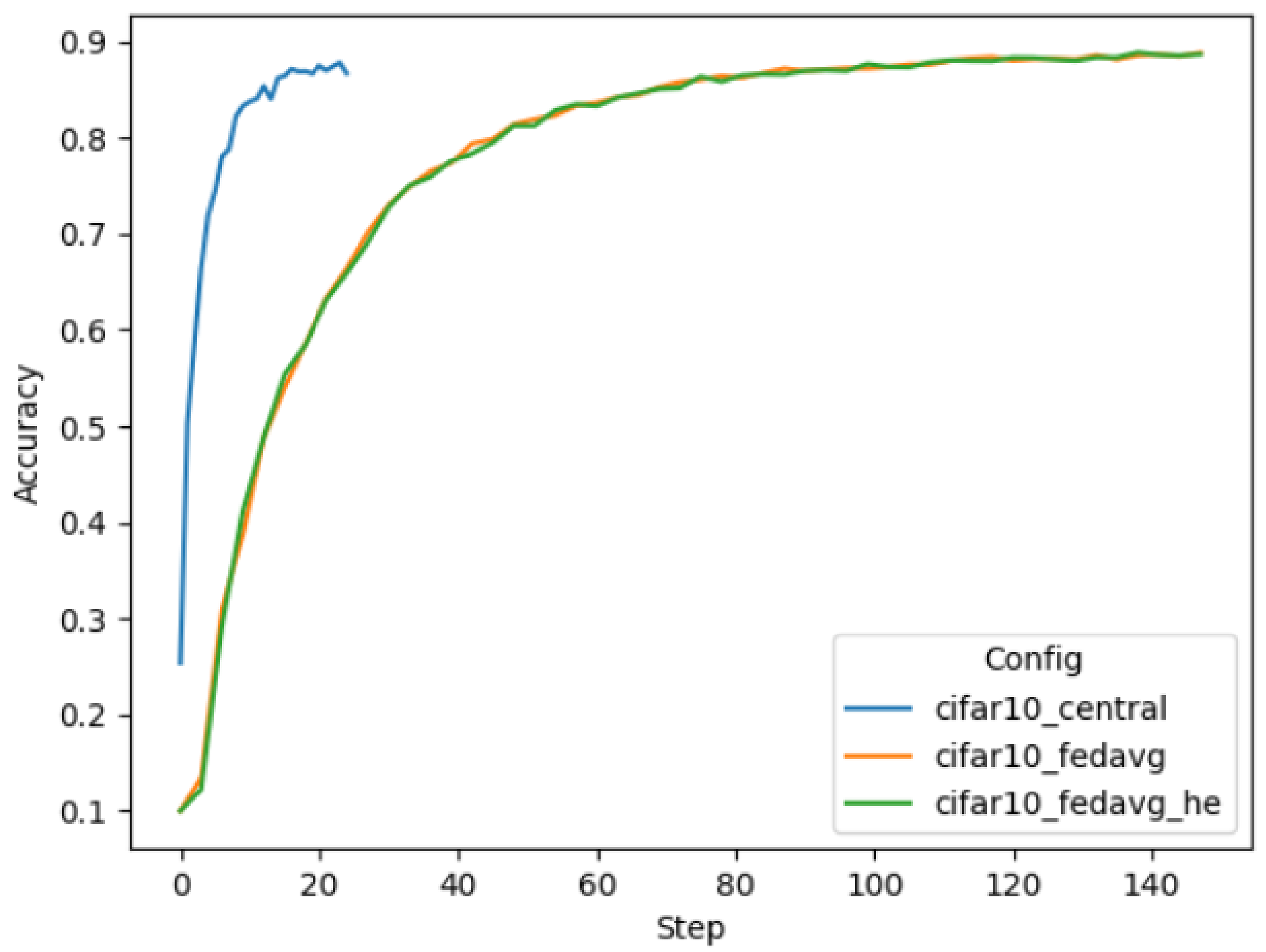




4.1 Central vs. FedAvg

With a data split using `alpha=1.0`, i.e. a non-heterogeneous split, we achieve the follc achieve a similar performance to central training and that HE does not impact the per aggregation step.

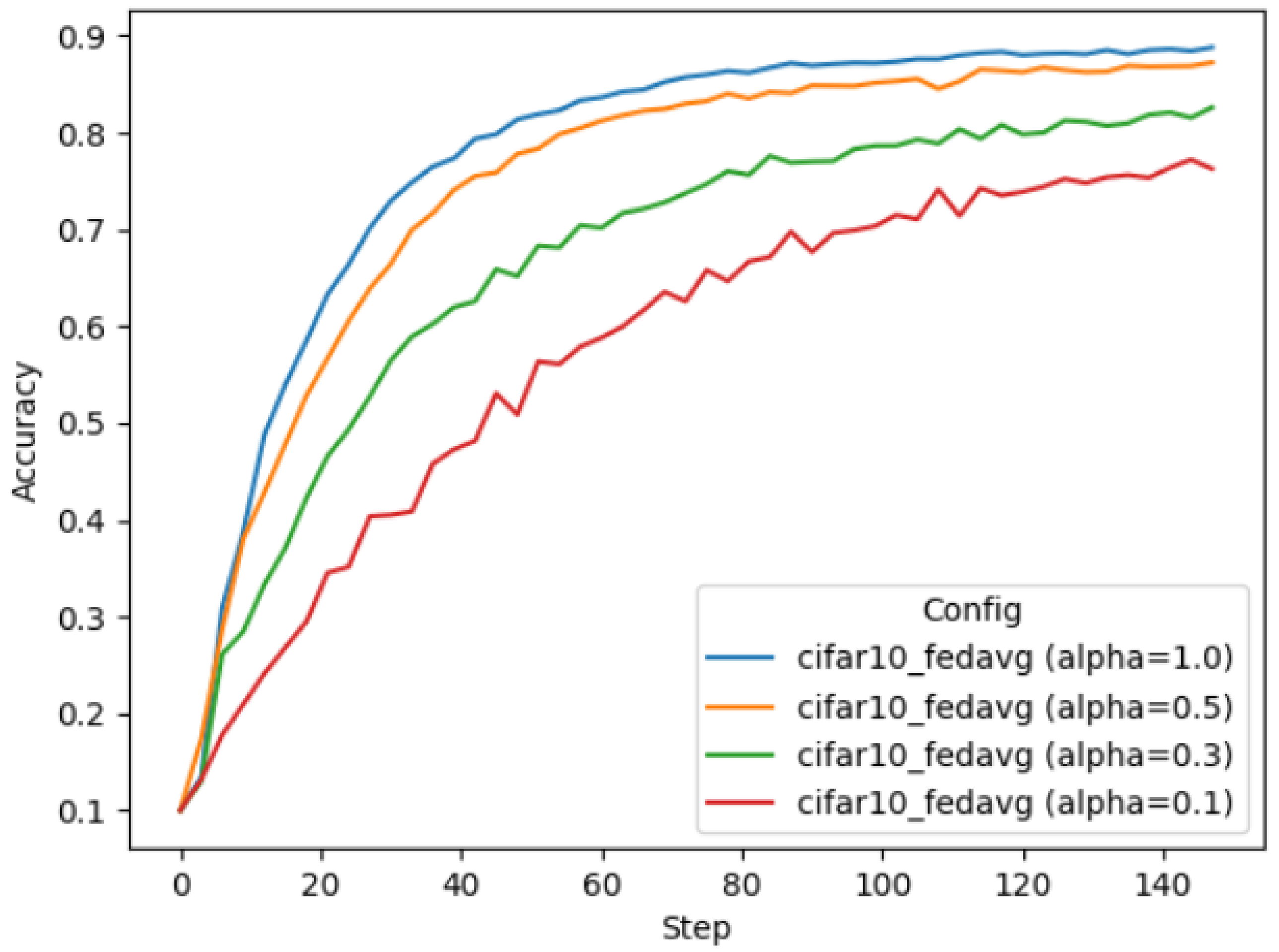
Config	Alpha	Val score
cifar10_central	1.0	0.8668
cifar10_fedavg	1.0	0.8840
cifar10_fedavg_he	1.0	0.8868



4.2 Impact of client data heterogeneity

We also tried different `alpha` values, where lower values cause higher heterogeneity. Thi FedAvg algorithms.

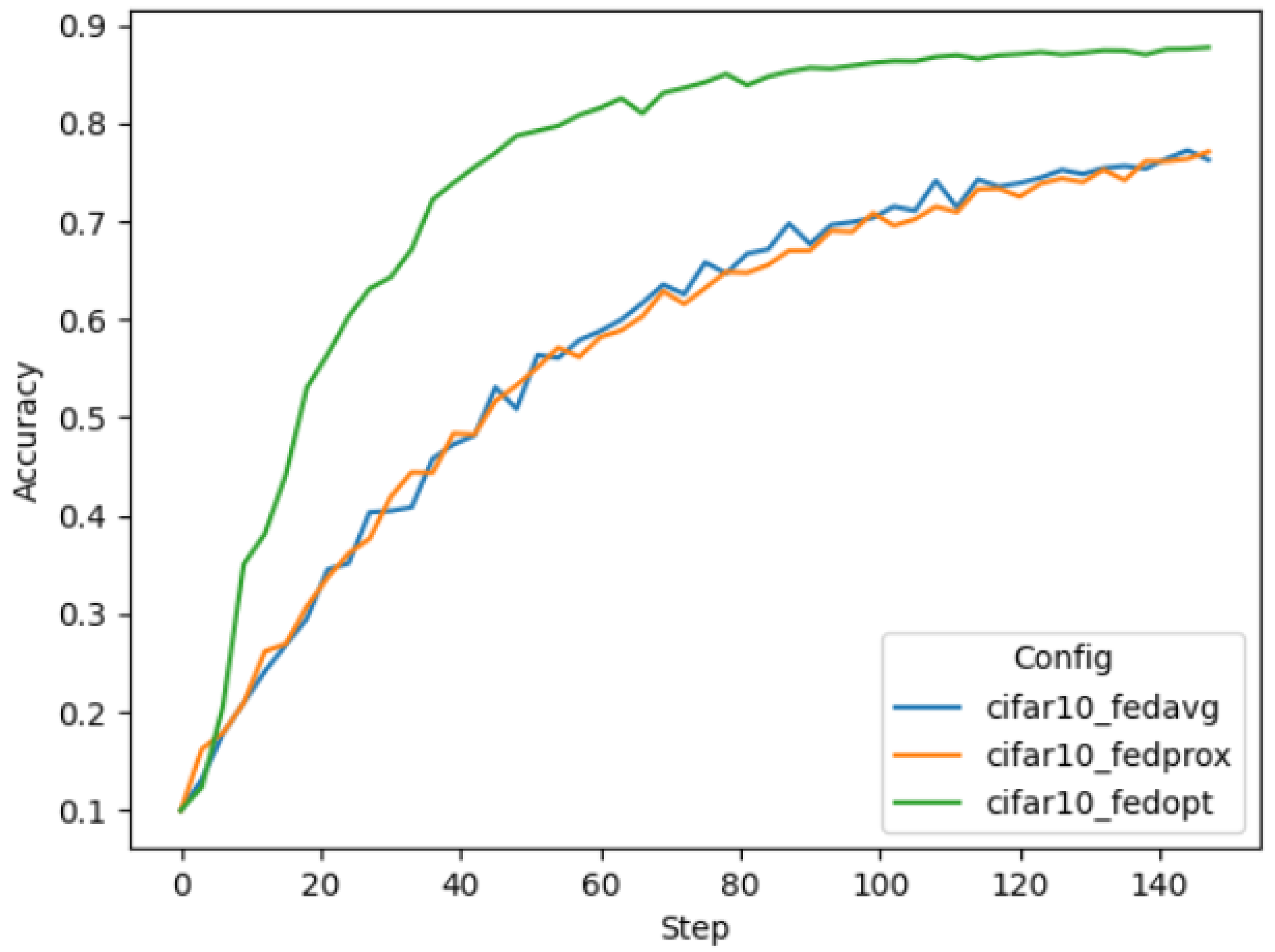
Config	Alpha	Val score
cifar10_fedavg	1.0	0.8840
cifar10_fedavg	0.5	0.8727
cifar10_fedavg	0.3	0.8264
cifar10_fedavg	0.1	0.7626



4.3 FedProx vs. FedOpt

Finally, we are comparing an `alpha` setting of 0.1, causing a high client data heteroç namely FedProx and FedOpt. Both achieve a better performance compared to FedAv convergence rate by utilizing SGD with momentum to update the global model on tl amount of training steps.

Config	Alpha	Val score
cifar10_fedavg	0.1	0.7626
cifar10_fedprox	0.1	0.7709
cifar10_fedopt	0.1	0.7963

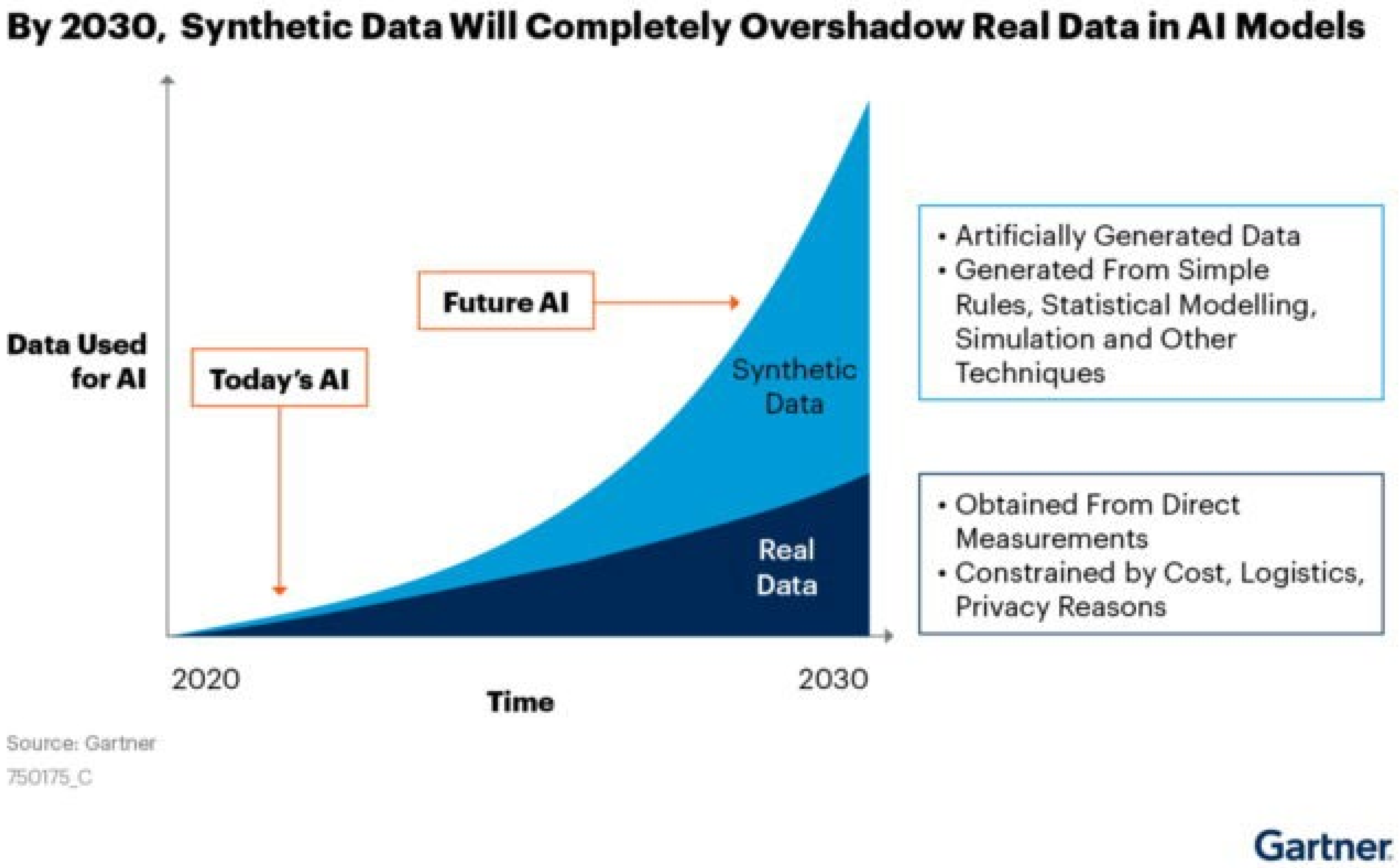


Synthetic data: Inherent Anonymization

> By 2030, synthetic data will completely overshadow real data in AI models.

Ramos & Subramanyam, Gartner Report 2021

Rise of Synthetic Data



https://blogs.nvidia.com/blog/2021/06/08/what-is-synthetic-data/

Source: Gartner, “Maverick Research: Forget About Your Real Data – Synthetic Data Is the Future of AI,” Leinar Ramos, Jitendra Subramanyam, 24 June 2021.

Synthetic data potentials and risks

Potentials

- Fake patient records and fake medical imaging is truly non-identifiable: no relation to real individuals
- Protect patient privacy and augment clinical research
- “A single image that could cost $6 from a labeling service can be artificially generated for six cents.” (Paul Walborsky, co-founder AI.Reverie, one of the first dedicated synthetic data services)
- Reducing bias by ensuring data diversity to represent the real world: Synthetic datasets are automatically labeled and can deliberately include rare but crucial corner cases

Risks

- Rise of companies monetising fake data and enabling cross-border data sharing beyond data protection legislation.
- No robust and objective methods of determining whether a synthetic dataset is sufficiently different from the original
- Example: Insurance companies buy and sell synthetic consumer data that is technically non-identifiable but retains all the properties of the original dataset required to adjust premiums for specific consumer groups.

Synthetic patient data in health care: a widening legal loophole

Anmol Arora • Ananya Arora

Published: March 28, 2022 •

DOI: https://doi.org/10.1016/S0140-6736(22)00232-X

https://doi.org/10.1016/s0140-6736(22)00232-x

Is the future of privacy synthetic?

14 July 2021

Thomas Zerdick, Head of Technology and Privacy

https://edps.europa.eu/press-publications/press-news/blog/future-privacy-synthetic_en

What Is Synthetic Data?

Synthetic data generated from computer simulations or algorithms provides an inexpensive alternative to real-world data that's increasingly used to create accurate AI models.

June 8, 2021 by GERARD ANDREWS

https://blogs.nvidia.com/blog/2021/06/08/what-is-synthetic-data/

Types of Deep Generative Models

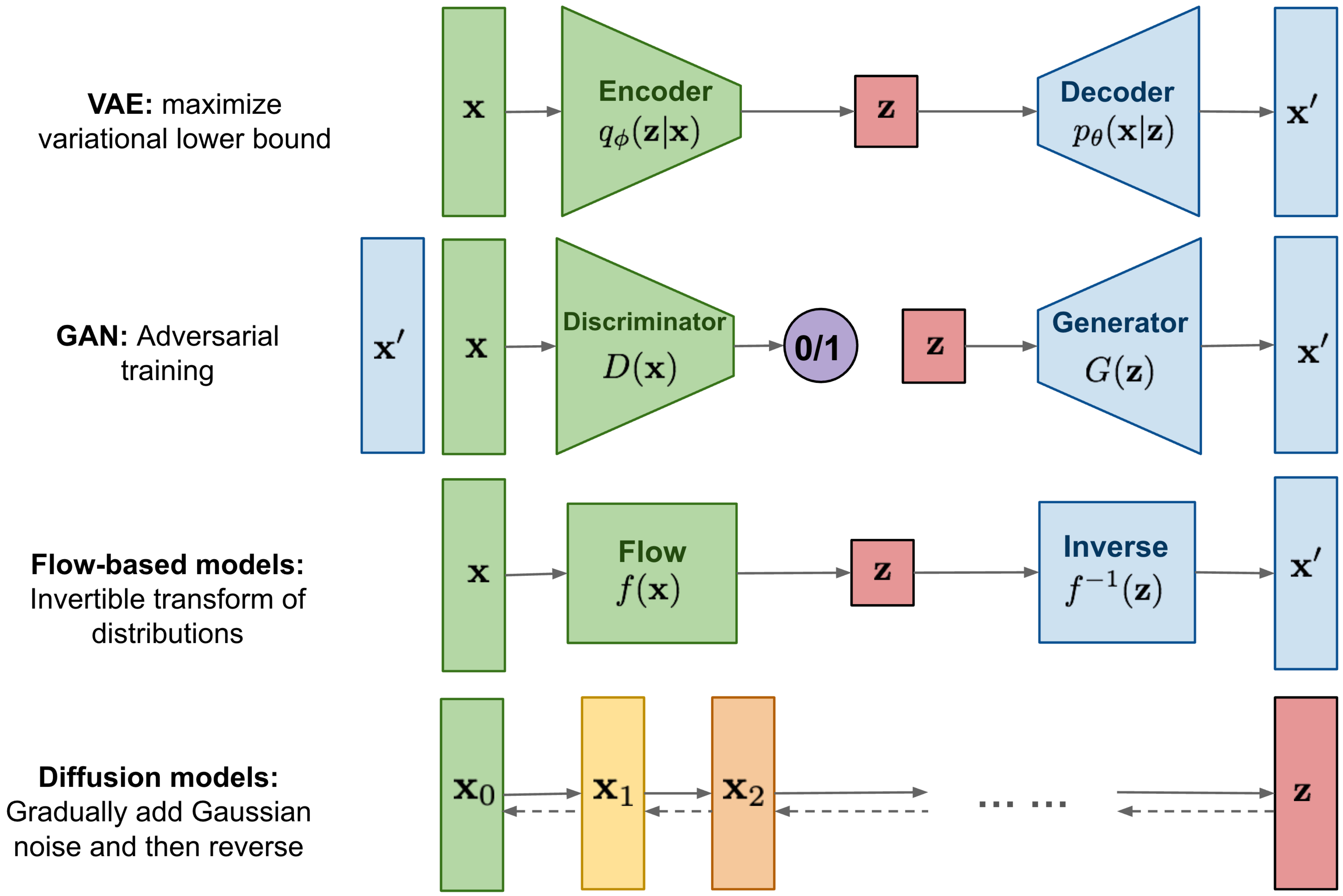


Figure source: https://lilianweng.github.io/posts/2021-07-11-diffusion-models/

Latest successes with Diffusion Models

A new paradigm: „Augmented Creativity“?

“An astronaut riding a horse in a photorealistic style.”

https://openai.com/dall-e-2/

OpenAI

“A brain riding a rocketship heading towards the moon.”

https://imagen.research.google/

Google

“Beautiful dress design for new york fashion week, 8k render in octane.”

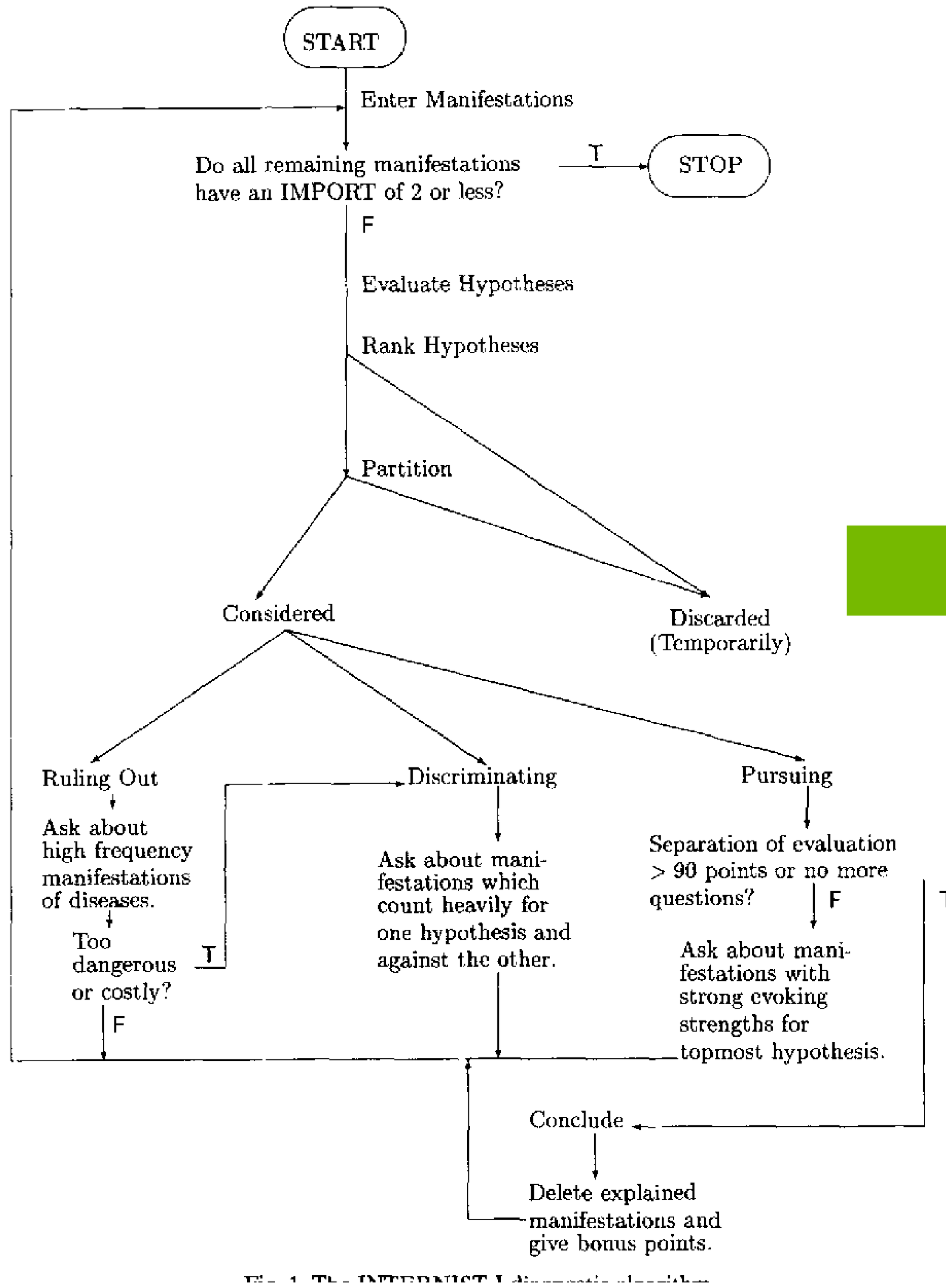
https://stability.ai/blog/stable-diffusion-public-release

stability.ai

Use Case: Synthetic Medical Cases

Curai Health

- Startup Curai trained a diagnostic model on 400,000 simulated medical cases
- Synthetic samples contained EHR data



INTERNIST-I computer-assisted diagnostic tool

Hepatitis acute viral

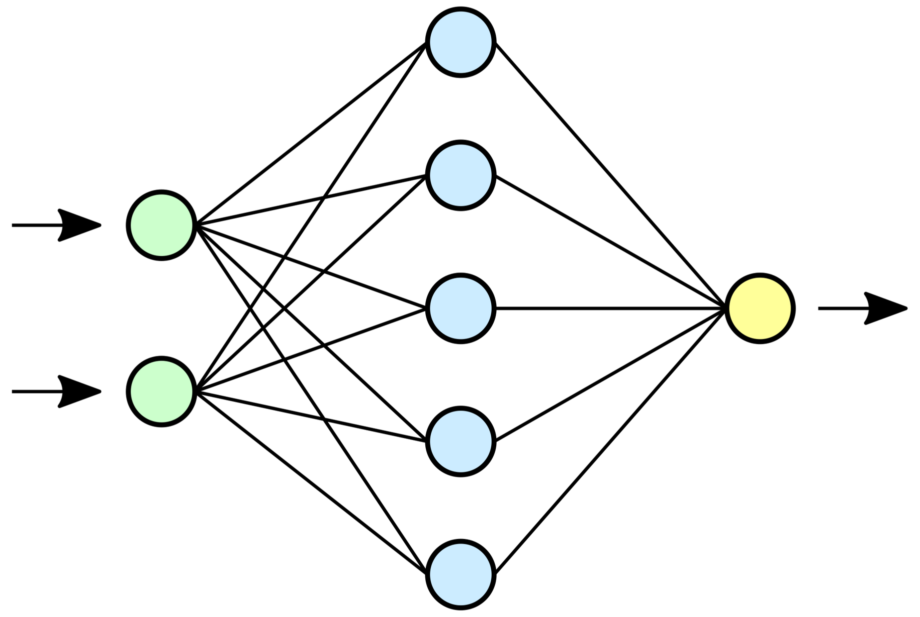
- jaundice, abdomen pain exacerbation with food, abdomen pain epigastrium, hepatomegaly present, liver enlarged moderate,liver tender on palpation, abdomen pain present, joint pain mild or moderate, abdomen tenderness present
- anorexia, jaundice, abdomen pain epigastrium, hepatomegaly present, liver enlarged moderate, liver tender on palpation, feces light colored, hands palmar erythema, skin spider angiomas, abdomen pain acute, abdomen pain present, abdomen pain not colicky, vomiting recent, constipation, vomiting coffee grounds

Arthritis acute septic

- joint tenderness swelling redness, joint involvement polyarticular asymmetrical, hip pain unilateral or bilateral, joint pain severe, joint range of motion decreased, knee pain unilateral or bilateral, joint effusions single or multiple, onset abrupt, fever, joint exam abnormal
- tachycardia, joint exam abnormal, joint tenderness swelling redness, joint pain severe, joint range of motion decreased, knee pain unilateral or bilateral, joint effusions single or multiple, joint involvement monoarticular, onset abrupt, shoulder pain left, shoulder pain right

Simulating medical cases from an expert knowledge base

ML model training



Test cases

Test time inputs to model	Approach			
	Expert	Probabilistic	LR	DNN
symptom	0.33 (0.56)	**0.43 (0.66)**	0.15 (0.26)	0.32 (0.47)
history	0.36 (0.54)	**0.48 (0.69)**	0.12 (0.21)	0.38 (0.53)
history and symptom	0.48 (0.67)	**0.62 (0.79)**	0.46 (0.43)	0.54 (0.69)
sign	0.58 (0.79)	0.67 (0.85)	0.30 (0.66)	**0.72 (0.88)**
history and sign	0.65 (0.84)	0.77 (0.91)	0.59 (0.76)	**0.86 (0.95)**
sign and symptom	0.62 (0.82)	0.71 (0.88)	0.59 (0.79)	**0.82 (0.95)**
history, sign and symptom	0.71 (0.88)	0.82 (0.94)	0.73 (0.89)	**0.92 (0.98)**

Ravuri, M., Kannan, A., Tso, G. J., & Amatriain, X. (2018, November). Learning from the experts: From expert systems to machine-learned diagnosis models. In Machine Learning for Healthcare Conference (pp. 227-243). PMLR.

Use Case: NLP from Synthetic Clinical Text

UF UNIVERSITY of FLORIDA

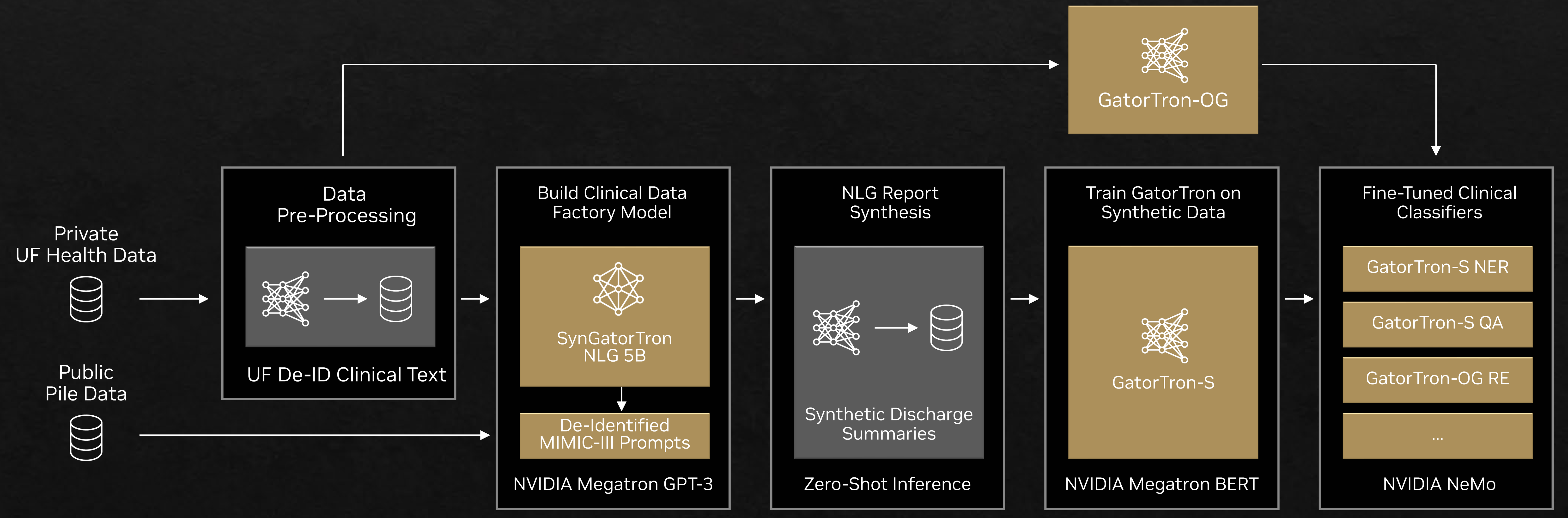
NVIDIA

University Florida and NVIDIA create World's largest clinical generative NLP models

SynGatorTron, GatorTron

- Clinical Language Generation Model SynGatorTron NLG 5B
- Used to generate synthetic, de-identified clinical notes and reports
- Trained GatorTron-S with synthetic data
- GatorTron–S achieves equivalent SOTA as original GatorTron-OG

UFHealth
UNIVERSITY OF FLORIDA HEALTH



	Results NER: Named Entity Recognition		**Results RE:** Relation Extraction		**Results QA:** Question Answering	
Synthetic data:	Gatortron-S	0.8893	Gatortron-S	0.9601	Gatortron-S	72.75
Original data:	Gatortron-OG	0.8859	Gatortron-OG	0.9599	Gatortron-OG	71.81

Available on NGC:

https://catalog.ngc.nvidia.com/orgs/nvidia/teams/clara/models/gatortron_og

https://catalog.ngc.nvidia.com/orgs/nvidia/teams/clara/models/gatortron_s

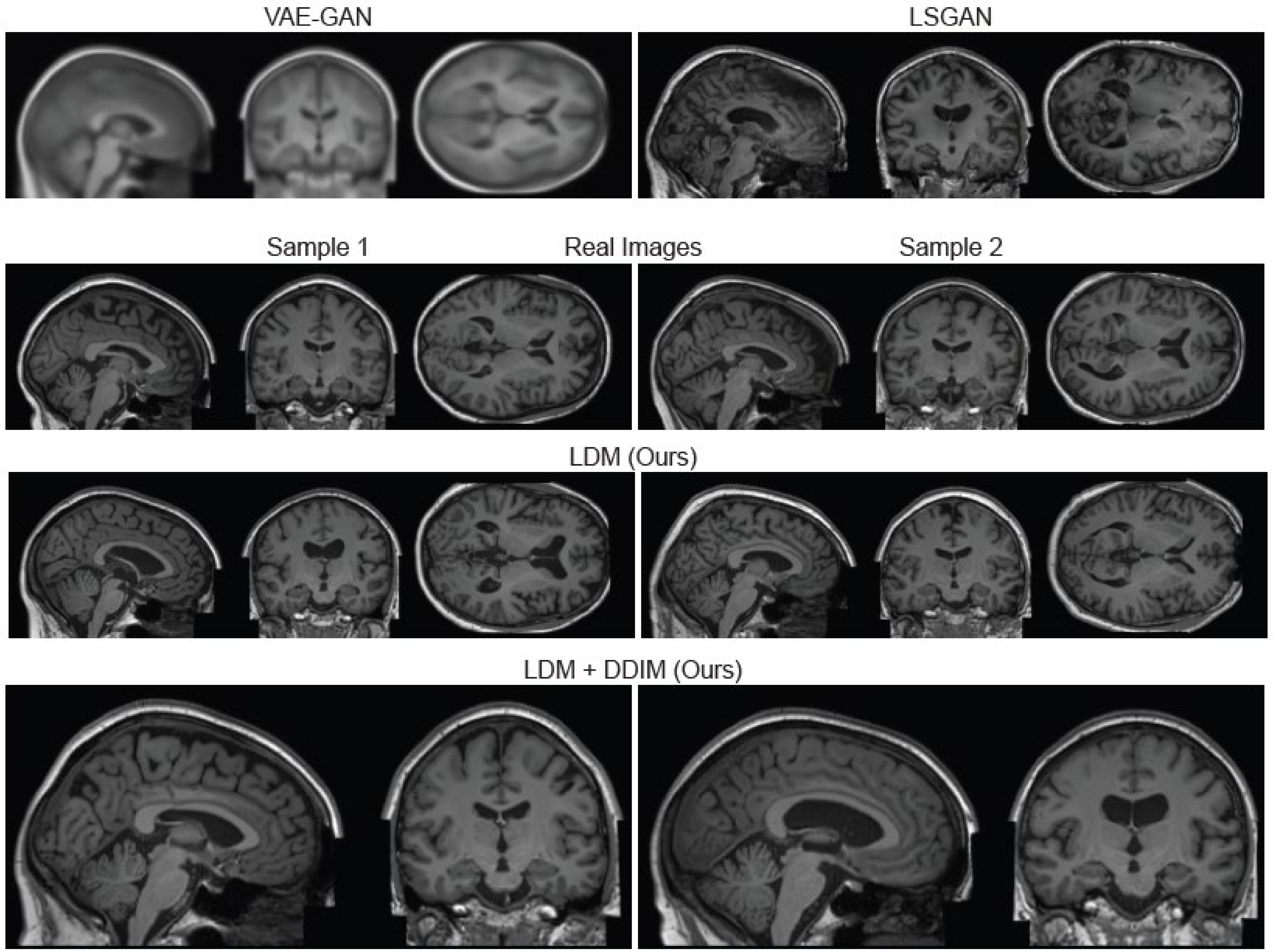
"With the help of large language model training technologies in NVIDIA Megatron, the University of Florida trained both 5B and 20B parameter clinical GPT-3 models. The 20B parameter model was trained in just 20 days on 70 DGX-A100 80GB nodes on their HiPerGator-AI SuperPOD system.
These models produce high fidelity, naturally de-identified clinical free text data for use in training downstream models without the risks of revealing protected health information or complexities of accessing and de-identifying hospital system electronic health records."

https://blogs.nvidia.com/blog/2022/03/22/uf-health-syngatortron-ai-synthetic-clinical-data/

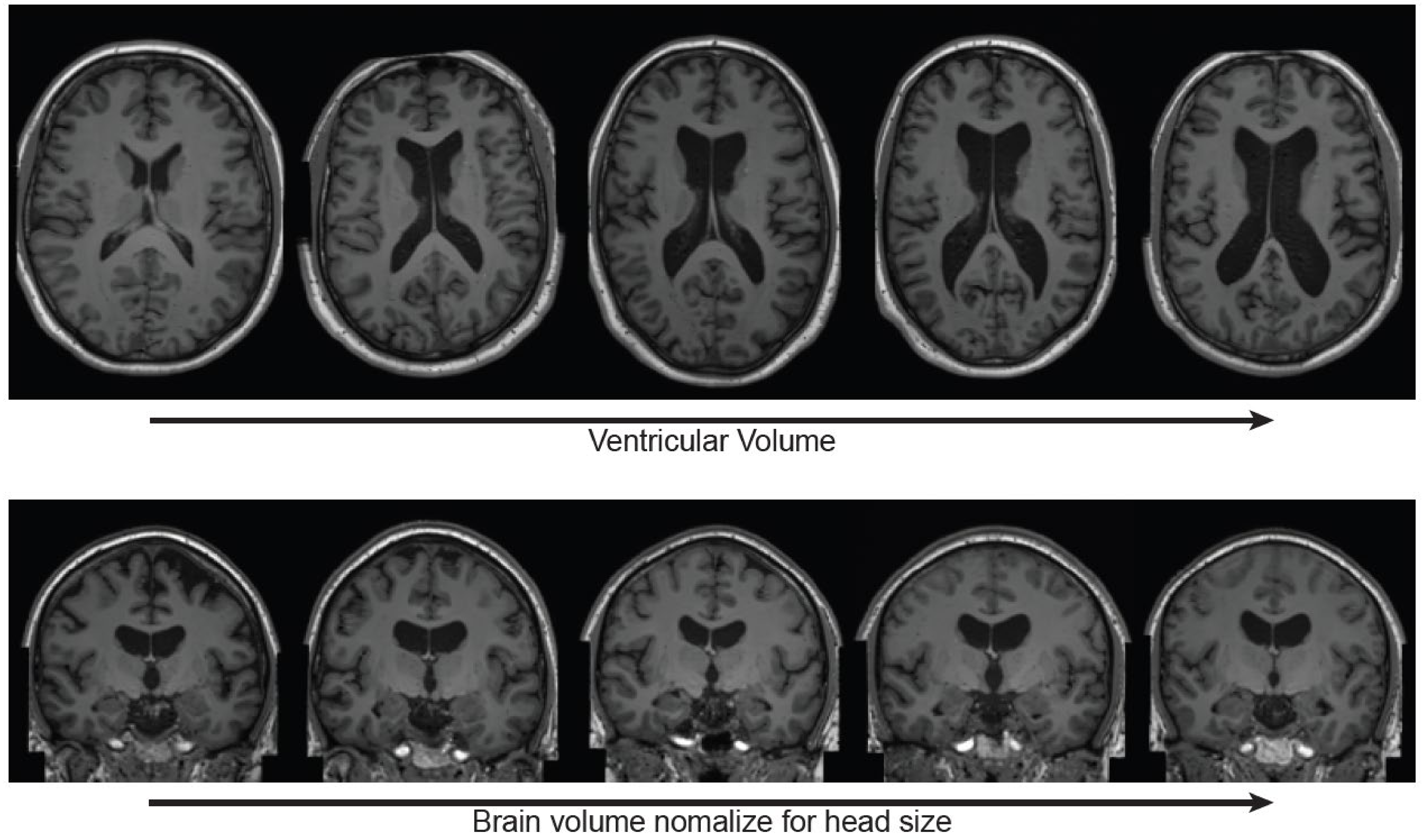
Use Case: 100.000 Synthetic T1w-MRI Brain Scans

Generation with Conditional Latent Diffusion Models (LDM)

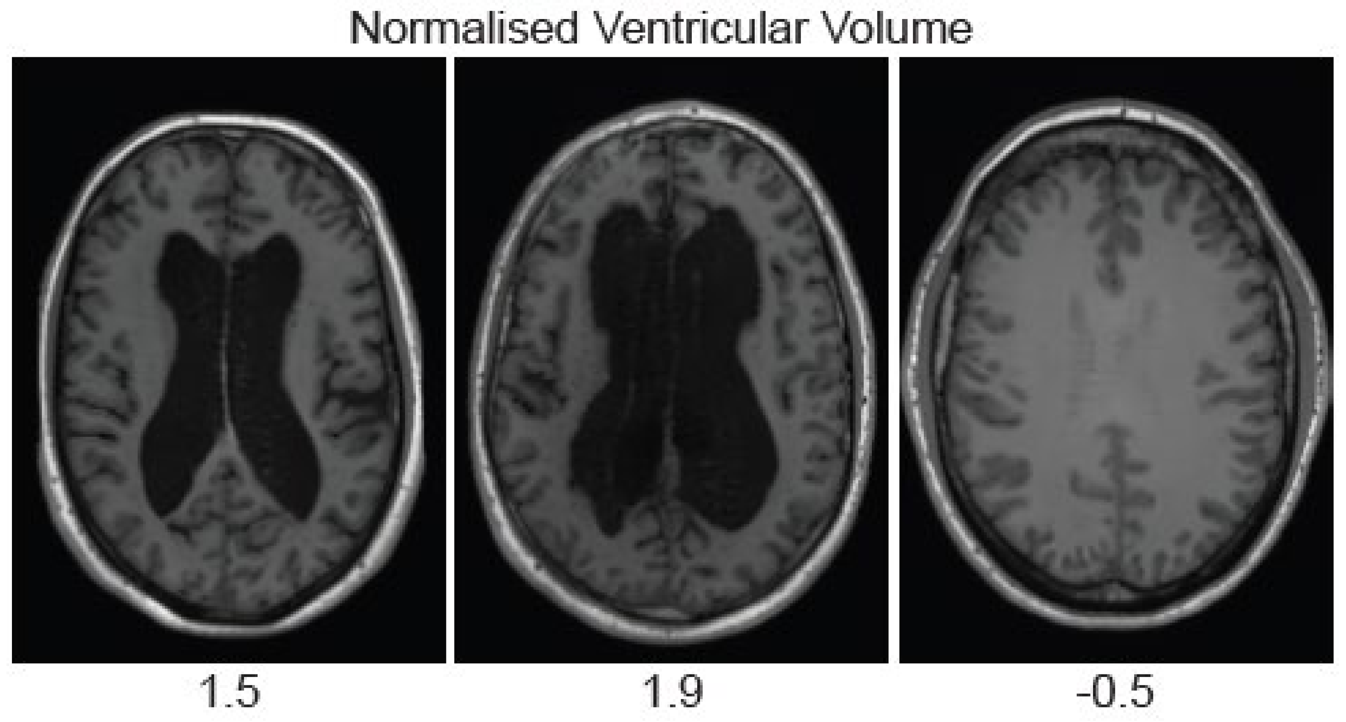
Generation



Conditioning



Extrapolation



Pinaya, W.H.L. et al. (2022). Brain Imaging Generation with Latent Diffusion Models. In: Mukhopadhyay, A., Oksuz, I., Engelhardt, S., Zhu, D., Yuan, Y. (eds) Deep Generative Models. DGM4MICCAI 2022. Lecture Notes in Computer Science, vol 13609. Springer, Cham.
Paper: https://doi.org/10.1007/978-3-031-18576-2_12, https://arxiv.org/abs/2209.07162
LDM 100k Dataset: https://academictorrents.com/details/63aeb864bbe2115ded0aa0d7d36334c026f0660b

Trained on NVIDIA Cambridge-1

UK's Fastest Supercomputer

1st Dedicated Industrial Supercomputer for Health

#42 on Top500 Supercomputers

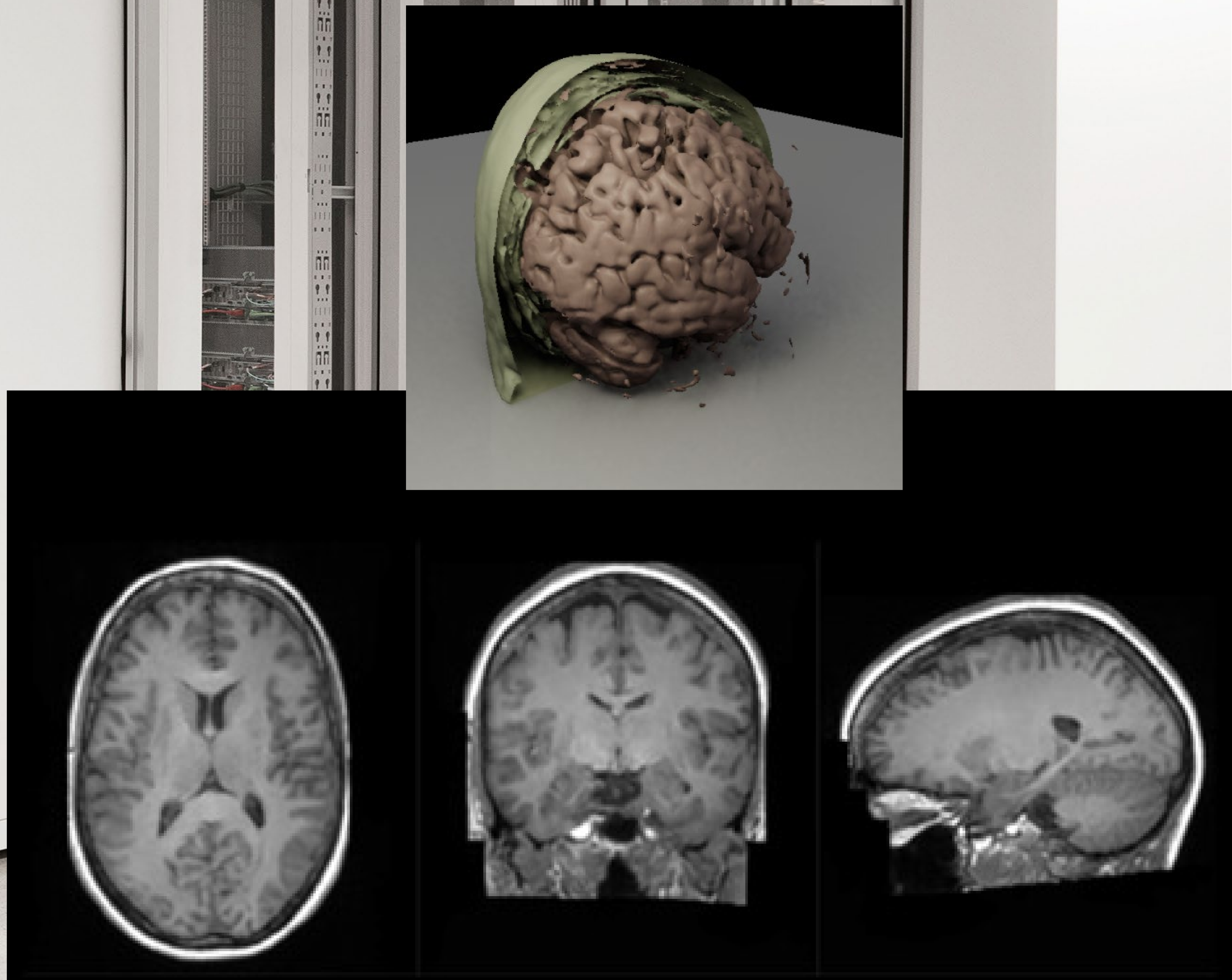
100% Powered by Renewable Energy

80 DGX A100 Nodes

640 NVIDIA A100 Universal GPUs

400 Petaflops AI Compute

NVIDIA



Synthetic Brain 3D Image Creation
NVIDIA + King's College London

Summary

Summary

Towards robust AI in healthcare without jeopardizing patient privacy

- **Modern machine and deep learning are data-hungry!**
  - Insufficient data can cause overfitting and therefore poor generalization to new/unseen cases
- **Data sharing under de-identification:**
  - Necessary to develop robust AI models, to reduce bias, and to improve data diversity (e.g. of minorities and of rare diseases)
  - Contra sharing: de-identification is always imperfect
    - Multiple sparse data sources can be combined to achieve patient re-identification ()
    - Modern ML algorithms exacerbate this weakness (e.g. face/voice/gait detectors)
    - For every engineered de-identification, a new re-identification method may pop up (e.g. brainprint)
  - Pro sharing:
    - Data sharing is a matter of contributing to the common good: "If I want to benefit from someone else's data, I have a duty to also share my own." (Nigam Shah, Stanford Institute for Human-Centered AI)
    - In practice, large-scale de-identification attacks have not been observed.
- **Federated Learning (FL):**
  - Share the model, not the data! Securely tapping into down data silos across institutions.
  - NVIDIA FLARE: Open-source FL SDK for fast-track entry into FL topics
- **Synthetic data with deep generative models:**
  - Inherent anonymity with steerable data diversity.
- **Democratization of AI:**
  - Open-source software frameworks improve accessibility, reproducible research and safety of algorithms!

NVIDIA

Towards robust AI in healthcare without jeopardizing patient privacy

Dr. Seyed-Ahmad Ahmadi
NVIDIA Senior Solution Architect, Deep Learning in Healthcare

Workshop “Responsible ML for Healthcare”
Oct 27, 2022, Copenhagen, DK

PIONEER CENTRE FOR ARTIFICIAL INTELLIGENCE

DANMARKS FRIE FORSKNINGSFOND

DDSA